Mathematics of the Rubik's cube

Associate Professor W. D. Joyner

Spring Semester, 1996–7

"By and large it is uniformly true that in mathematics that there is a time lapse between a mathematical discovery and the moment it becomes useful; and that this lapse can be anything from 30 to 100 years, in some cases even more; and that the whole system seems to function without any direction, without any reference to usefulness, and without any desire to do things which are useful."

John von Neumann
COLLECTED WORKS, VI, p. 489

For more mathematical quotes, see the first page of each chapter below, [M], [S] or the www page at http://math.furman.edu/~mwoodard/mquot.html

"There are some things which cannot
be learned quickly, and time, which is all we have,
must be paid heavily for their acquiring.
They are the very simplest things,
and because it takes a man's life to know them
the little new that each man gets from life
is very costly and the only heritage he has to leave."

Ernest Hemingway
(From A. E. Hotchner, PAPA HEMMINGWAY, Random House, NY, 1966)

Contents

Illustrations in this text (jpg files):

chapter 2:
VENN1.JPG
box2.JPG

chapter 3:
plotf1b.jpg
plotf2b.jpg

chapter 4:
15a1.jpg
15b1.jpg
15c1.jpg
circles1.JPG
equator1.JPG
ball3.jpg
ball4.jpg
ball5.jpg
box4.jpg
box3.jpg
skewb4.jpg
tetra2.jpg
tetra4.jpg
penta1.jpg
penta2.jpg

chapter 5:
square2.jpg
cube2.jpg
hexa1.jpg
bells3.jpg

chapter 6:
cayley1.jpg
cayley2.jpg
icosian.jpg
15puzz1.jpg

15puzz3.jpg
15puzz9.jpg and 15puzz6.jpg
15puzz2.jpg
15puzz10.jpg and 15puzz11.jpg
15puzz4.jpg and 15puzz5.jpg

chapter 7:
tetra3.jpg
octah2.jpg
dodec2.jpg
icosah2.jpg
icosah3.jpg
icosah4.jpg

chapter 8:
none

chapter 9:
groups1.JPG
coxeter2.JPG

chapter 10:
rubike1.jpg, rubike2.jpg, rubike3.JPG
rubiko1.jpg, rubiko2.jpg
sqr1c.JPG
sqr1a.JPG and sqr1b.jpg

chapter 11:
none

chapter 12:
cube1.jpg
crossgp.jpg

chapter 13, 14:
none

Chapter 0

Introduction

> "The advantage is that mathematics is a field in which one's blunders tend to show very clearly and can be corrected or erased with a stroke of the pencil. It is a field which has often been compared with chess, but differs from the latter in that it is only one's best moments that count and not one's worst."
>
> *Norbert Wiener*
> *EX-PRODIGY: MY CHILDHOOD AND YOUTH*

Groups measure symmetry. No where is this more evident than in the study of symmetry in 2- and 3-dimensional geometric figures. Symmetry, and hence groups, play a key role in the study of crystallography, elementary particle physics, coding theory, campanology (see §5.11 below), and the Rubik' s cube, to name just a few.

This is a book biased towards learning group theory not learning to solve "the cube". To paraphrase the German mathematician David Hilbert, the art of doing group theory is to pick a good example to learn from. The Rubik's cube will be our example. We motivate the study of groups by creating a group-theoretical model of Rubik's cube-like puzzles. Although some solution strategies are discussed (for the 15 puzzle, the Rubik's cube - the $3\times3\times3$ and $4\times4\times4$ versions, the "Rubik tetrahedron" or pyraminx, the "Rubik dodecahedron" or megaminx, the skewb, square 1, the masterball, and the equator puzzle), these are viewed more abstractly than most other books on the subject. We regard a solution strategy merely as a reasonably

efficient algorithm for constructing any element in the associated group of moves.

The approach here is different than some other group theory presentations (such as Rotman [R]) in that

(a) we emphasize puzzle-related group theoretical examples over general theory,

(b) we present some of the basic notions algorithmically (as in [Bu]), and

(c) we tried to keep the level as low as possible for as long as possible (though only the reader can judge if we've keep it low enough long enough, or too low too long!).

The hope is that by following along and doing as many of the exercises as possible the reader will have fun learning about how groups can be used to solve a "real life" problem (assuming you consider solving the Rubik's cube a problem from real life!). Along the way, we shall also explain the rules of a two person game (the Gordon game) which arises from group theory - a game which arises from a group not a group which arise from a game. See also the superflip game introduced in §4.5.2 (related to coin-turning games of H. W. Lenstra) and W. Hamilton's Icosian game in §6.2.1. This is probably one of the few mathematics texts which contains an exercise of the form: "Play a game!".

Experience has shown that in order to keep up a pace which allows the class to finish the proof of the "fundamental theorems of cube theory" (see §4.5.2 and §10.2) in one semester, the students should either (a) be candidates for the honors program or (b) have some group-theoretical background. More modest goals might be more appropriate for classes with less background.

Acknowledgements: Many of the graphs given below were produced with the help of MAPLE. Some of the group-theoretical calculations (such as the order of a group element) were determined with the help of GAP. The contributions from students were a big help. I especially thank my former students Gen Gomes, Ann Luers, Jim McShea, Justin Montague, and Spencer Robinson for their help and collaboration on some of the topics. I'd also like to thank Andy Southern for collaborating on some of the masterball material [JS] which appears in chapter 14 and Dennis Spellman for the argument in §9.7 where a presentation of wreath products is derived.

Chapter 1

Logic and sets

> "If logic is the hygiene of the mathematician, it is not his source of food; the great problems furnish the daily bread on which he thrives."
>
> *Andre Weil*
>
> *"The future of mathematics", AMER MATH MONTHLY, May, 1950*

> "The rules of logic are to mathematics what those of structure are to architecture."
>
> *Bertrand Russell*
>
> *MYSTICISM AND LOGIC AND OTHER ESSAYS, 1917, p61*

This chapter will present some background to make some of the terminology and notation introduced later a little clearer. It is not intended to be a rigorous introduction to mathematical logic.

1.1 Logic

A statement is a logical assertion which is either true or false. (Of course we assume that this admitedly circular 'definition' is a statement.) Sometimes the truth or falsity of a statement is called its Boolean value. One can combine several statements into a single statement using the connectives 'and', 'or', and 'implies'. The Boolean value of a statement is changed using the 'negation'. We shall also use 'if and only if' and 'exclusive or' but these can

be defined in terms of negation $\sim$ and the other three connectives ($\vee$, $\wedge$, and $\Rightarrow$).

Exercise 1.1.1. Do this. In other words, express $\_\vee$ and $\iff$ in terms of $\sim$, $\vee$, $\wedge$, and $\Rightarrow$.

Notation: Let p and q be statements.

statement	notation	terminology
p and q	p $\wedge$ q	"conjunction"
p or q	p $\vee$ q	"disjunction"
p implies q	p $\Rightarrow$ q	"conditional"
negate p	$\sim$p	"negation"
p if and only if q	p $\iff$ q	"if and only if"
either p or q (not both)	p $\_\vee$ q	"exclusive or"

Truth tables: Given the Boolean values of p, q, we can determine the values of $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \iff q$, $p\_ \wedge q$ using the truth tables:

p	q	p $\wedge$ q
T	T	T
T	F	F
F	T	F
F	F	F

p	q	p $\vee$ q
T	T	T
T	F	T
F	T	T
F	F	F

p	q	p $\Rightarrow$ q
T	T	T
T	F	F
F	T	T
F	F	T

p	q	p $\iff$ q
T	T	T
T	F	F
F	T	F
F	F	T

p	q	p $\_\vee$ q
T	T	F
T	F	T
F	T	T
F	F	F

p	$\sim$ p
T	F
F	T

Exercise 1.1.2. (M. Gardner) Determine which of the following statements is true.

- Exactly one of these statements is false.
- Exactly two of these statements are false.
- Exactly three of these statements are false.
- Exactly four of these statements are false.
- Exactly five of these statements are false.
- Exactly six of these statements are false.
- Exactly seven of these statements are false.
- Exactly eight of these statements are false.
- Exactly nine of these statements are false.
- Exactly ten of these statements are false.

Definition 1. Let B be the set $\{0, 1\}$ with the two operations addition (+) and multipication (*) defined by the following tables

p	q	p + q
1	1	0
1	0	1
0	1	1
0	0	0

p	q	p * q
1	1	1
1	0	0
0	1	0
0	0	0

(Note how these mimic the truth tables of 'exclusive or' ($\_\vee$) and 'and' ($\wedge$).) We call B the Boolean algebra.

Exercise 1.1.3. Use truth tables to verify DeMorgan's laws:
(a) $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$,
(b) $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$,
and the laws of negation:
(c) $\sim (p \wedge q) \iff (\sim p) \vee (\sim q)$,
(d) $\sim (p \vee q) \iff (\sim p) \wedge (\sim q)$.
(You may want to do (a), (c), (d) first, then deduce (b) from these.)

Definition 2. A logical argument is a sequence of statements (called hypotheses) $p_1, p_2, ..., p_n$, which imply a statement q (called the conclusion).

In other words, a logical argument is a true statement of the form

$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \Rightarrow q.$$

Exercise 1.1.4. Use truth tables to verify the logical argument

$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r).$$

Definition 3. 'For all', written $\forall$, is the universal quantifier. 'There exists', written $\exists$, is the existential quantifier.

A variable is a letter denoting some (possibly unknown) object. A constant is a letter denoting some specific, well-defined object. A term is a variable or constant.

A predicate is a function

$$P : \{terms\} \rightarrow \{logical\ statements\}.$$

Example 4. 'Daffy Duck' is a constant. 'x and Daffy Duck are cartoon characters' is a predicate involving a variable and a constant.

1.1.1 Expressing an everyday sentence symbolically

When creating a model of the Rubik's cube, we shall of course need to convert some 'everyday statements' into symbolical form in order to perform mathematical analysis. Let's illustrate this with an example.

Example 5. Consider the statement "Each student in this class is a mathematics major". Let

$$M(x) = x \text{ is a mathematics major}, \qquad S(x) = x \text{ is a student in this class.}$$

The symbolic form is

$$\forall x,\ S(x) \Rightarrow M(x).$$

Exercise 1.1.5. Convert "Someone in this class likes the Rubik's cube" to symbolic form.

Exercise 1.1.6. (M. Gardner [Gar2]) Professor White, Professor Brown and Professor Black were lunching together. "Isn't it remarkable", said the lady, "that our names are White, Black, and Brown and one of us has black hair, one has brown hair, and one has white hair."

"It is indeed", answered the one with the black hair as Professor Black bit into his sandwich, "and have you noticed that not one has hair color to match our name?"

The lady's hair is not brown. What is the color of Professor Black's hair?

	white	brown	black	lady
White				
Brown				
Black				
lady				×

1.2 Sets

A set is a 'well-defined' collection of objects. The objects in a set are the elements of the set.

There are two common ways to describe a set:

(a) list all its elements (if the set is finite, e.g., $\{1, 2, 3\}$),

(b) describe the set using properties of its elements (e.g., the set of all even integers can be described by $\{n \mid n \text{ an integer}, \ 2 \text{ divides } n\}$).

Remark 1. We must be a little careful when describing sets using properties since some 'self-referential' properties lead to contraditions: let

$$R = \{x \mid x \notin x\}.$$

In other words, for all x, $x \in R \iff x \notin x$. In particular, if we take $x = R$ then this becomes

$$R \in R \iff R \notin R,$$

an obvious contradition. The problem is that R is not "well-defined" (in the sense that it does not satisfy the set-theoretic axioms which we will skip here).

The empty set is the set containing no elements, denoted $\emptyset$.

Notation: Let S and T be sets. Assume that $S \subset X$.

statement	notation	terminology
set of elements in S and T	$S \cap T$	intersection
set of elements in S or T	$S \cup T$	union
set of elements in S or T (not both)	$S \Delta T$	symmetric difference
set of elements not in S	S^c	complement
S is a subset of T	$S \subset T$	subset

Exercise 1.2.1. Use Venn diagrams to verify the DeMorgan laws:
(a) $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$,
(b) $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$,
and the laws of negation:
(c) $(S \cap T)^c = S^c \cup T^c$,
(d) $(S \cup T)^c = S^c \cap T^c$.

Definition 6. We call two sets S, T disjoint if they have no elements in common, i.e., if

$$S \cap T = \emptyset.$$

If

$$S = \cup_{i=1}^{n} S_i,$$

where the $S_1, S_2, ..., S_n$ are pairwise disjoint sets then we call this union a partition of S.

Example 7. If

$$S = \mathbb{Z}, \quad S_1 = \{..., -2, 0, 2, ...\} = \text{even integers},$$

$$S_2 = \{..., -3, -1, 1, 3, ...\} = \text{odd integers},$$

then $S = S_1 \cup S_2$ is a partition of the integers into the set of even and odd ones.

Logic/set theory analogs: Just as one can use connectives to form new statements from old statements, there are analogous ways to form new sets from old ones using 'intersection' (the analog of 'and'), 'union' (the analog of 'or'), and 'complement' (the analog of 'negation'). The analog of 'implies' is 'subset'.

set theory	logic
sets	statements
union	or
intersection	and
subset	implies
symmetric difference	exclusive or
equal	if and only if
Venn diagrams	truth tables

For more on logic or set theory, see for example [C] or [St].

Chapter 2

Functions, matrices, relations and counting

> "I think mathematics is a vast territory. The outskirts of mathematics are the outskirts of mathematical civilization. There are certain subjects that people learn about and gather together. Then there is a sort of inevitable development in those fields. You get to a point where a certain theorem is bound to be proved, independent of any particular individual, because it is just in the path of development."
>
> *William P. Thurston*
> *MORE MATHEMATICAL PEOPLE, NY, 1990, p332*

> "Chance favors the prepared mind."
>
> *Louis Pasteur*

This chapter will introduce some frequently used notions.

2.1 Functions

Let S and T be finite sets.

Definition 8. : A function f from S to T is a rule which associates to each element $s \in S$ exactly one element $t \in T$. We will use the following notations

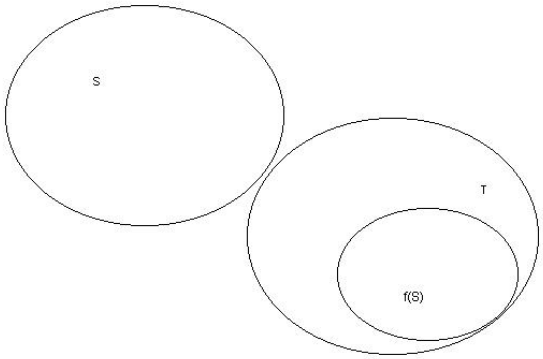
for this:

$$f : S \to T \quad (\text{"f is a function from S to T"}),$$
$$f : s \longmapsto t \quad (\text{"f sends s in S to t in T"}),$$
$$t = f(s) \quad (\text{"t is the image of s under f"}).$$

A function is also called a map, mapping, or transformation. We call S the domain of f, T the range of f, and the set

$$f(S) = \{f(s) \in T \mid s \in S\}$$

the image of f. The Venn diagram depicting this setup is:



The Cartesian product of two sets S, T is the set of pairs of elements taken from these sets:

$$S \times T = \{(s, t) \mid s \in S, t \in T\}.$$

Example 9. If $\mathbb{R}$ denotes the set of all real numbers then the Cartesian product $\mathbb{R} \times \mathbb{R}$ is simply the plane of pairs of real numbers we are all familiar with.

More generally, we may iterate this process and take the Cartesian product the set of real numbers with itself n times (where $n > 1$ is any integer) to get $\mathbb{R} \times ... \times \mathbb{R}$ (n times). This n-fold Cartesian product is denoted more conveniently by $\mathbb{R}^n$. An element of the set $\mathbb{R}^n$ will be called a vector or an n-vector to be specific.

The graph of a function $f : S \to T$ is the subset

$$\{(s, f(s) \mid s \in S\} \subset S \times T.$$

It is not possible for every subset of $S \times T$ the graph of some function from S to T. The following fact classifies exactly which subsets of $S \times T$ can arise as the graph of a function from S to T.

Lemma 10. *: Let $X \subset S \times T$. X is the graph of a function from S to T if and only if, for all $(s_1, t_1) \in X$ and $(s_2, t_2) \in X$, whenever $t_1 \neq t_2$ we also have $s_1 \neq s_2$.*

Exercise 2.1.1. Verify this. (Hint: Let

$$\begin{array}{c} pr_1 : S \times T \to S \\ (s,t) \longmapsto s \end{array}$$

be projection onto the 1st component. Recall that the graph of a function has the property that $pr_1^{-1}(s)$ is always a singleton.)

Definition 11. If the image of the function $f : S \to T$ is all of T, i.e., if $f(S) = T$, then we call f <u>surjective</u> (or "onto", or "is a surjection").

Equivalently, a function f from S to T is surjective if each t in T is the image of some s in S under f. Occasionally, you see the following special notation for surjective functions:

$$f : S \twoheadrightarrow T \qquad (f \text{ "maps } S \text{ surjectively onto } T\text{"}).$$

Exercise 2.1.2. State a general rule which determines those subsets X of $S \times T$ which are the graph of some surjective function from S to T. (Use the projection onto the second component,

$$\begin{array}{c} pr_2 : S \times T \to T \\ (s,t) \longrightarrow t \end{array}$$

in your rule.)

Question: Suppose that $|S| < |T|$. Is there a *surjective* function $f : S \to T$? Explain.

Definition 12. : A function $f : S \to T$ is called <u>injective</u> (or "one-to-one" or "an injection") if each element t belonging to the image $f(S)$ is the image of exactly one s in S.

In other words, f is an injection if the condition $f(s_1) = f(s_2)$ (for some $s_1, s_2 \in S$) always forces $s_1 = s_2$. Sometimes the "hook arrow" notation is used to denote an injective function

$$f : S \hookrightarrow T.$$

Question: Suppose that $|S| > |T|$. Is there an injective function $f : S \to T$? Explain.

Exercise 2.1.3. Suppose that $|S| = |T|$. Show that a function $f : S \to T$ is surjective if and only if it is injective.

Definition 13. A function $f : S \to T$ is called a bijection if it is both injective and surjective.

Equivalently, a bijection from S to T is a function for which each t in T is the image of exactly one s in S.

Exercise 2.1.4. Give an algorithm for determining if a given finite subset X of $S \times T$ is the graph of a bijection from S to T.

Definition 14. A set S is called countable if there exists a bijection $f : S \to \mathbb{Z}$ to the set of integers $\mathbb{Z}$.

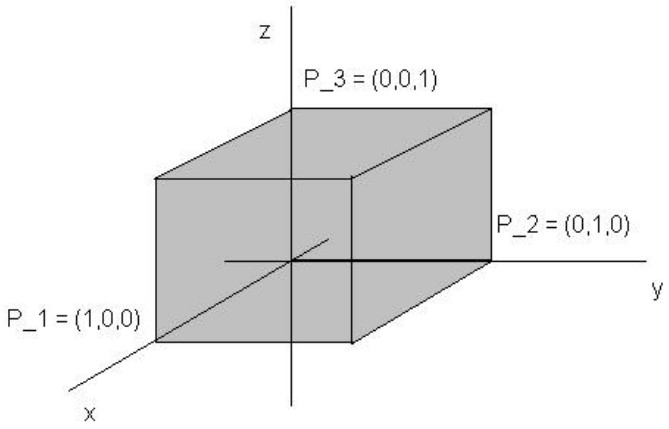
Example 15. The set S of all rational numbers $0 < r < 1$ is countable since you can define $f : S \to \mathbb{Z}$ as follows: $f(1) = 1/2$, $f(2) = 1/3$, $f(3) = 2/3$, $f(4) = 1/4$, $f(5) = 3/4$, $f(6) = 1/5$, $f(7) = 2/5$, $f(8) = 3/5$, and so on. There are $\phi(n)$ terms of the form m/n, where m is relatively prime to n and $\phi(n)$ denotes the number of positive integers less than or equal to n which are relatively prime to n (i.e., have no common prime divisors). (ϕ is sometimes called Euler's phi function).

Exercise 2.1.5. Give an algorithm for determining if a given *finite* subset X of $S \times T$ is the graph of a bijection from S to T.

Example 16. Let C be the cube in 3-space having vertices at the points $O = (0,0,0), P_1 = (1,0,0), P_2 = (0,1,0), P_3 = (0,0,1), P_4 = (1,1,0), P_5 = (1,0,1), P_6 = (0,1,1), P_7 = (1,1,1)$. We shall also (to use a notation which will be used more later) denote these by dbl, dfl, dbr, ubl, dfr, ufl, ubr, ufr, resp. Let $C_0 = \{O, P_1, ..., P_7\}$ be the set of the 8 vertices of C, let $C_1 = \{uf, ur, ub, ul, fr, br, bl, fl, df, dr, db, dl\}$ be the set of the 12 edges of C, and let $C_2 = \{F, B, U, B, L, R\}$ be the set of the 6 faces of C. Let r be

the rotation of a point (x, y, z) by 180 degrees about the passing through the points $(1/2, 1/2, 0)$, $(1/2, 1/2, 1)$. Note that $r : \mathbb{R}^3 \to \mathbb{R}^3$ is a function which sends the cube C onto itself.

The cube C is pictured as follows:



This function r induces three functions

$$f_0 : C_0 \to C_0, \quad f_1 : C_1 \to C_1, \quad f_2 : C_2 \to C_2.$$

where f_i is the function which sends $x \in C_i$ to its image $r(x)$ under r (which is again in C_i), for $i = 0, 1, 2$. Each f_i is a bijection.

Exercise 2.1.6. Finish the labeling of the vertices and the faces in the above picture and describe f_1 and f_2 explicitly by filling out the tables

v	$f_0(v)$	e	$f_1(e)$	f	$f_2(f)$

Lemma 17. *If $f : S \to T$ is a bijection then there exists a function $f^{-1} : T \to S$ defined by the following property: for $s \in S$ and $t \in T$, we have*

$$f^{-1}(t) = s \qquad \text{if and only if } f(s) = t.$$

Exercise 2.1.7. Prove this.

Definition 18. The function f^{-1} in the above lemma is called the inverse function of f.

2.2 Functions on vectors

This section presents a few basic facts about matrices, which we regard as a certain type of function which sends vectors to vectors. For further details, see any text on linear algebra, for example [JN] where the historical introduction below is borrowed from.

2.2.1 History

The mathematician who first published a major work which seriously studied matrices and matrix algebra in the western world was Lord Arthur Cayley (1821-1895) of Cambridge, England. He wrote a memoir on the theory of linear transformations which was published in 1858 and is often thought of as one of the "fathers" of matrix theory, though in fact it was his friend and colleague James Sylvester who first coined the term "matrix".

Here is one of the earliest examples which motivated Cayley: if we have three coordinate systems $(x, y), (x', y')$, and (x'', y'') , connected by

$$\begin{cases} x' = x + y \\ y' = x - y \end{cases}$$

and

$$\begin{cases} x'' = -x' - y' \\ y'' = -x' + y' \end{cases}$$

then the relationship between (x, y) and (x'', y'') is given

$$\begin{cases} x'' = -x' - y' = -(x + y) - (x - y) = -2x \\ y'' = -x' + y' = -(x + y) + (x - y) = -2y \end{cases}$$

If we do as Cayley did and abbreviate the three change of coordinates by the square array of the coefficients then we obtain the three arrays

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}.$$

Cayley noticed that there was an algebraic rule which allows us to determine the third array from the first two, without doing the substitution we did above to relate (x'', y'') to (x, y). This rule involves the rows of the first array and the columns of the second array. For example, to get the entry in the upper left-hand corner of the third array, Cayley explained we need to combine the first row of the first array with the first column of the second array as follows: $-2 = 1 \cdot (-1) + 1 \cdot (-1)$. (The general formula will be given below.) To get the entry in the upper right-hand corner of the third array, we combine the first row of the first array with the second column of the second array: $0 = 1 \cdot (-1) + 1 \cdot 1$. To get the entry in the lower left-hand corner of the third array, we combine the second row of the first array with the first column of the second array: $0 = 1 \cdot (-1) + (-1) \cdot (-1)$. Finally, to get the entry in the upper left-hand corner of the third array, we combine the first row of the first array with the first column of the second array: $-2 = 1 \cdot (-1) + (-1) \cdot 1$. The relationship which we just described betweeen the about three arrays he called "matrix multiplication".

2.2.2 3×3 matrices

First, a 3×3 matrix is a 3×3 table of real numbers

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

which acts on $\mathbb{R}^3$ by matrix multiplication:

$$A\vec{v} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_{11}x + a_{12}y + a_{13}z \\ a_{21}x + a_{22}y + a_{23}z \\ a_{31}x + a_{32}y + a_{33}z \end{pmatrix}$$

In general, any such 3×3 matrix gives rise to a function $A : \mathbb{R}^3 \to \mathbb{R}^3$.

Example 19. If $A = I_3$, the 3×3 identity matrix,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then $I_3\vec{v} = \vec{v}$ for all $\vec{v} \in \mathbb{R}^3$.

2.2.3 Matrix multiplication, inverses

An $m \times n$ matrix (of real numbers) is a rectangular array or table of numbers arranged with m rows and n columns. It is usually written:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

The $(i,j)^{th}$ entry of A is a_{ij}. The ith row of A is

$$\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{bmatrix} \qquad (1 \le i \le m)$$

The jth column of A is

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix} \qquad (1 \le j \le n)$$

A matrix having as many rows as it has columns ($m = n$) is called a square matrix. The square $n \times n$ matrix

$$\begin{pmatrix} 1 & & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & & 0 \\ 0 & \vdots & 0 & 1 \end{pmatrix}$$

is called the $n \times n$ identity matrix and denoted I or I_n.

2.2.4 Muliplication and inverses

You can multiply an $m \times n$ matrix A by a $n \times p$ matrix B and get a $m \times p$ matrix AB. The $(i,j)^{th}$ entry of AB is computed as follows:

1. Let $k = 1$ and $c_0 = 0$.
2. If $k = m$, you're done and $a_{ij} = c_m$. Otherwise proceed to the next step.
3. Take the k^{th} entry of the i^{th} row of A and multiply it by the k^{th} entry of the j^{th} row of B. Let $c_k = c_{k-1} + a_{ik}b_{kj}$.
4. Increment k by 1 and go to step 2.

In other words, multiply each element of row i in A with the corresponding entry of column j in B, add them up, and put the result in the (i,j) position of the array for AB.

If A is a square $n \times n$ matrix and if there is a matrix B such that $AB = I_n$ then we call B the inverse matrix of A, denoted A^{-1}.

2.3 Relations

A relation on a set is a generalization of the concept of a function from S to itself.

Definition 20. : Let S be a set. If R is a subset of $S \times S$ then we call R a relation on S. If $(x,y) \in R$ then we say that x is related to y.

We may also regard a relation R on S as a function

$$R : S \times S \to \{0,1\}.$$

In this form, we say x is related to y (for $x, y \in S$) if $f(x,y) = 1$.

This is a very general notion. There are lots and lots of relations in mathematics - inequality symbols, functions, subset symbols are all common examples of relations.

Example 21. Let S be any set and let f be a function from S to itself. This function gives rise to the relation R on S defined by the graph of f:

$$R = \{(x,y) \in S \times S \mid y = f(x), \text{ for } x \in S\}.$$

(It is through this correspondence that we may regard a function as a relation.)

Example 22. Let S be the set of all subsets of $\{1, 2, ..., n\}$. Let R be defined by

$$R = \{(S_1, S_2) \mid S_1 \subset S_2,\ S_1 \in S,\ S_2 \in S\}.$$

Note that R is a relation.

Exercise 2.3.1. Find a relation corresponding to the symbol $<$ on the real line.

Definition 23. Let R be a relation on a set S. We call R an equivalence relation if

(a) any element $s \in S$ is related to itself ("reflexive"),

(b) if s is related to t (i.e., (s, t) belongs to S) then t is related to s ("symmetry"),

(c) if s_1 is related to s_2 and s_2 is related to s_3 then s_1 is related to s_3 ("transitivity").

Example 24. The equality symbol $=$ provides an equivalence relation on the real line: let $D = \{(x, x) \mid x \text{ real}\}$. This is an equivalence relation on the real line: note $x = y$ if and only if (x, y) belongs to D.

Notation: If R is an equivalence relation on S then we often write $x \sim y$ or $x \equiv y$ in place of $(x, y) \in R$, for simplicity.

Example 25. Fix an integer $n > 1$. For integers x, y, define $x \equiv y$ if and only if n divides $x - y$. In this case, we say that x is congruent to y mod n. The equivalence class of x is sometimes (for historical reasons) called the residue class (or congruence class) of x mod n. This notation was first introduced by Gauss [1]

Exercise 2.3.2. (a) Let $f(x) = x^2$, let S be the real line, and let R be the corresponding relation as in the first example. Is R an equivalence relation?

(b) Let $f(x) = 2x$, let S be the real line, and let R be the corresponding relation as in the first example. Is R an equivalence relation?

[1] C. F. Gauss, 1777-1855, is regarded by many as one of the top mathematicians of all time. At the age of 21 he wrote "Disquisitiones Arithmeticae", which started a new era of number theory and introduced this notation.

Exercise 2.3.3. Let R be the corresponding relation as in the second example. Is R an equivalence relation?

Let R be an equivalence relation on a set S. For $s \in S$, we call the subset

$$[s] = \{t \in S \mid s \sim t\}$$

the equivalence class of s in S.

Example 26. For integers x, y, define $x \equiv y$ if and only if 3 divides $x - y$. the equivalence classes are

$$[0] = \{..., -6, -3, 0, 3, 6, ...\},$$
$$[1] = \{..., -5, -2, 1, 4, 7, ...\},$$
$$[2] = \{..., -4, -1, 2, 5, 8, ...\}.$$

Exercise 2.3.4. Show that for any s_1 and s_2 in S, we have either
(a) $[s_1] = [s_2]$, or
(b) $[s_1]$ is disjoint from $[s_2]$.

As a consequence of this exercise, we see that if R is an equivalence relation on a set S then the equivalence classes of R partition S into disjoint subsets. We state this as a separate lemma for future reference (we also assume S is finite for simplicity):

Lemma 27. *: If S is a finite set and R is an equivalence relation on S then there are subsets*

$$S_1 \subset S,\ S_2 \subset S, ..., S_k \subset S,$$

satisfying the following properties:
(1) S is the union of all the S_i's:

$$S = S_1 \cup S_2 \cup ... \cup S_k = \cup_i S_i$$

(2) the S_i's are disjoint: for $1 \leq i \leq k$, $1 \leq j \leq k$, if $i \neq j$ then $S_i \cap S_j = \emptyset$.
(These last two properties say that the S_i's partition S in the sense of the previous chapter.)
(3) the S_i's exhaust the collection of equivalence classes of R: for each $1 \leq i \leq k$, there is an $s_i \in S$ such that

$$S_i = [s_i].$$

(This element s_i is called a representative of the equivalence class S_i.)

Example 28. For real numbers x, y, define $x \equiv y$ if and only if $x - y$ is an integer. The equivalence classes are of the form

$$[x] = \{..., x-2, x-1, x, x+1, x+2, ...\},$$

for x real. Each equivalence class has exactly one representative in the half open interval $[0, 1)$.

Remark 2. Conversely, given a partition as in (1), there is an equivalence relation R such that $S_i = [s_i]$, for some some $s_i \in S$, where

$$[s] = \{x \in S \mid s \sim x\}$$

is the equivalence class of s with respect to R. Indeed, we define

$$R = \cup_{i=1}^{k} S_i \times S_i.$$

This is an equivalence relation and $s \sim t$ if and only if $s, t \in S_i$, for some $i = 1, 2, ..., k$.

Exercise 2.3.5. Let S be the set $\mathbb{Z}$ of all integers. Let R be the relation defined by $(x, y) \in R$ if and only if $x - y$ is an even number (i.e., an integer multiple of 2).

(1) Show that this is an equivalence relation,
(2) Find the sets S_i in the above lemma which partition S,
(3) Find a representative of each equivalence class S_i.

2.4 Counting

This section quickly surveys the few basic counting principles we shall use later.

Addition principle: Let $S_1, ..., S_n$ denote disjoint finite sets. Then

$$|S_1 \cup ... \cup S_n| = |S_1| + ... + |S_n|.$$

Example 29. If there are n bowls, each containing some distinguishable marbles and if S_i is the set of marbles in the i^{th} bowl then the number of ways to pick a marble from exactly one of the bowls is $|S_1| + ... + |S_n|$, by the addition principle.

Corollary 30. *(Pigeonhole principle) If there are n objects (pigeons) which must be placed in m ($md < n$) boxes (pigeonholes) then there is at least one box with at least $d + 1$ objects.*

Example 31. If you are in a room with 9 others then there must be either at least 5 people you know or 5 people you don't know (not counting yourself). In this case, there are $n = 9$ objects and $m = 2$ boxes (the friend box and the stranger box) so we may take $d = 4$ in the pigeonhole principle.

Multiplication principle: Let $S_1, ..., S_n$ denote finite sets. Then

$$|S_1 \times ... \times S_n| = |S_1| \cdot ... \cdot |S_n|.$$

Example 32. If there are n bowls, each containing some distinguishable marbles and if S_i is the set of marbles in the i^{th} bowl then the number of ways to pick exactly one marble from each of the bowls is $|S_1| \cdot ... \cdot |S_n|$, by the multiplication principle.

Corollary 33. *The number of ordered selections, taken without repetition, of m objects from a set of n objects ($m < n$) is*

$$\frac{n!}{(n-m)!} = n \cdot (n-1) \cdot ... \cdot (n-m+1).$$

Corollary 34. *The number of ordered selections, taken with repetition allowed, of m objects from a set of n objects ($m < n$) is n^m.*

Example 35. The number of n-tuples, without repetition, of objects from the set $\{1, 2, ..., n\}$ is

$$n! = n \cdot (n-1) \cdot ... \cdot 1.$$

Exercise 2.4.1. Let C be a set of 6 distinct colors. Fix a cube in space (imagine it sitting in front of you on a table). We call a coloring of the cube a choice of exactly one color per side. Let S be the set of all colorings of the cube. We say $x, y \in S$ are equivalent if x and y agree after a suitable rotation of the cube.

(a) Show that this is an equivalence relation.

(b) Count the number of equivalence classes in S.

Chapter 3

Permutations

"What we have to learn to do, we learn by doing"
Aristotle
ETHICS

"Mathematics, springing up from the soil of basic human experience with numbers and data and space and motion, builds up a far-flung architectural structure composed of theorems which reveal insights into the reasons behind appearences and of concepts which relate totally disparate concrete ideas."
Sanders MacLane
AMER. MATH. MONTHLY, 1954

Let $T_n = \{1, 2, ..., n\}$ be the set of integers from 1 to a fixed positive integer n. When n is fixed and there is no ambiguity sometimes we will simply write T for T_n. A permutation of T is a bijection from T to itself. (A bijection was defined in Definition 13.) For example, on the 3×3 Rubik's cube there are $9 \cdot 6 = 54$ facets. If you label them $1, 2, ..., 54$ (in any way you like) then any move of the Rubik's cube corresponds to a permutation of T_{54}. In this chapter we present some basic notation and properties of permutations.

Notation: We may denote a permutation $f : T \to T$ by a $2 \times n$ array:

$$f \leftrightarrow \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}$$

Example 36. The identity permutation, denoted by I, is the permutation which doesn't do anything:

$$I = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

Definition 37. Let

$$e_f(i) = \#\{j > i \mid f(i) > f(j)\}, \qquad 1 \leq i \leq n-1.$$

Let

$$swap(f) = e_f(1) + ... + e_f(n-1).$$

We call this the swapping number (or length of the permutation f since it counts the number of times f swaps the inequality in $i < j$ to $f(i) > f(j)$. If we plot a bar-graph of the function f then $swap(f)$ counts the number of times the bar at i is higher than the bar at j. We call f even if $swap(f)$ is even and we call f odd otherwise.

The number

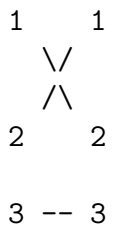
$$sign(f) = (-1)^{swap(f)}$$

is called the sign of the permutation f.

Example 38. Let $n = 3$, so $T = \{1, 2, 3\}$. We may describe the permutation $f : T \to T$ for which $f(1) = 2, f(2) = 1, f(3)$ by a 2×3 array

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

or by a "crossing diagram":



The number of crosses in this diagram is the swapping number of f, from which we can see that the permutation is odd.

Exercise 3.0.2. Express $f : T \to T$ given by $f(1) = 3, f(2) = 1, f(3) = 2$, as (a) a 2×3 array, (b) a crossing diagram. Find its swapping number and sign.

Definition 39. Let $f : T \to T$ and $g : T \to T$ be two permutations. We can compose them to get another permutation, the composition, denoted $fg : T \to T$:

$$\begin{array}{ccccc} t & \longmapsto & f(t) & \longmapsto & g(f(t)) \\ T & \to & T & \to & T \end{array}$$

Notation We shall follow standard convention and write our compositions of permutations **left-to-right**. (This is of course in contrast to the *right-to-left* composition of functions you may have seen in calculus.) When a possible ambiguity may arise, we call this type of composition "composition as permutations" and call "right-to-left composition" the "composition as functions".

When $f = g$ then we write ff as f^2. In general, we write the n-fold composition $f...f$ (n times) as f^n. Every permutation f has the property that there is some integer $N > 0$, which depends on f, such that $f^N = 1$. (In other words, if you repeatedly apply a permutation enough times you will eventually obtain the identity permutation.)

Definition 40. The smallest integer $N > 0$ such that $f^N = 1$ is called the order of f.

Example 41. Let $T = \{1, 2, 3\}$ and let

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

We have

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad f^2 = 1, \qquad g^3 = 1.$$

Exercise 3.0.3. Compute (a) fg and (b) the order of f and the order of g, where

$$(a) \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$(b) \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Exercise 3.0.4. If f, g, h are permutations of T, is $(fg)h = f(gh)$? Explain why.

3.1 Inverses

We can look at the graph of a function $f : T \to T$ and determine
(a) if it is injective,
(b) if it is surjective,
(c) the inverse f^{-1}, if it exists.
Indeed, from the graph of f we can determine the image $f(T)$ and this determines if f is surjective or not. The inverse exists only if f is injective (hence, in our case, surjective by exercise 2.1.3). It's graph is determined by reflecting the graph of f about the diagonal, x=y.

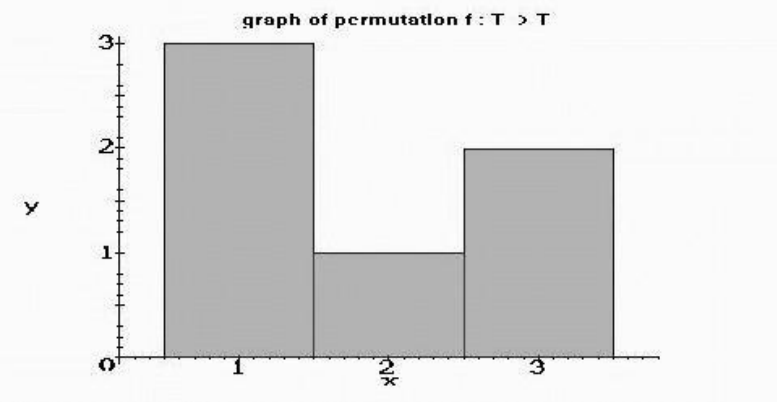
Lemma 42. *The following statements are equivalent:*
(1) $f : T \to T$ is injective,
(2) $f : T \to T$ is surjective,
(3) $|f(T)| = |T|$.

proof: The equivalence of the first two statements is by the exercise at the end of chapter 1. (2) is equivalent to (3), by definition of surjectivity. □

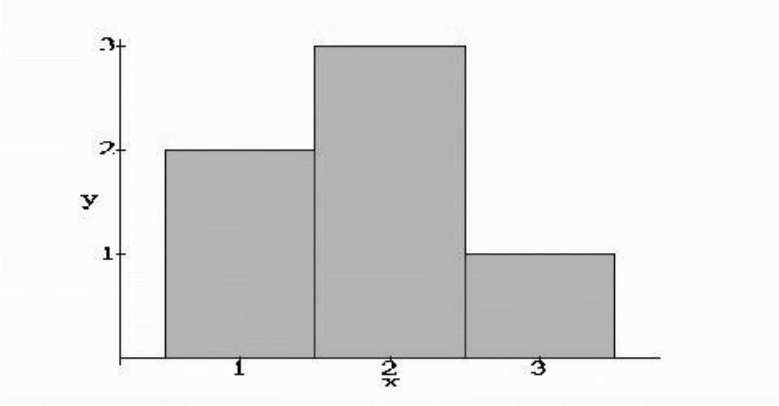
Example 43. The inverse of

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

is obtained by reflecting the graph



about the $x = y$ line:



Exercise 3.1.1. Graph and determine the inverses of the following permutations:

$$(a) \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$(b) \qquad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$(c) \qquad f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

There are two more commonly used ways of expressing a permutation. The first is the "matrix notation":

Definition 44. To a permutation $f : T \to T$, given by

$$f = \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}$$

we associate to it the matrix $P(f)$ of $0's$ and $1's$ defined as follows: the ij-th entry of $P(f)$ is 1 if $j = f(i)$ and is 0 otherwise.

(A brief introduction to matrices is given in the appendix.)

Definition 45. A square matrix which has exactly one 1 per row and per column (as $P(f)$ does) is called a permutation matrix .

Lemma 46. *There are* $n!$ *distinct* $n \times n$ *permutation matrices and there are* $n!$ *distinct permutations of the set* $\{1, 2, ..., n\}$.

Exercise 3.1.2. Prove this using the multiplication counting principle from the section on counting in the previous chapter.

Example 47. The matrix of the permutation f given by

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

is

$$P(f) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Note that matrix multiplication gives

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}$$

from which we can recover the 2×3 array.

Theorem 48. *If $f : T \to T$ is a permutation then*

$$(a) \qquad P(f) \begin{pmatrix} 1 \\ 2 \\ \vdots \\ n \end{pmatrix} = \begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{pmatrix}$$

Furthermore, the inverse of the matrix of the permutation is the matrix of the inverse of the permutation:

(b) $P(f)^{-1} = P(f^{-1})$,

and the matrix of the product is the product of the matrices:

(c) $P(fg) = P(f)P(g)$.

proof: If $\vec{v}$ is the column vector with entries $v_1, v_2, ..., v_n$ (the v_i are arbitrary real numbers) then $P(f)\vec{v}$ is the column vector whose i^{th} coordinate is equal to v_j if f sends i to j, by definition of $P(f)$. Since, in this case, $j = f(i)$ (here we write $f(i)$ to denote the image of i under the permutation f, ' even though i really gets plugged into f on the left), this implies that $P(f)\vec{v}$ is the column vector with entries $v_{f(1)}, v_{f(2)}, ..., v_{f(n)}$. This proves (a).

Note (b) is a consequence of (c) so we need only prove (c). We compute $P(fg)\vec{v}$ and $P(f)P(g)\vec{v}$. By the same reasoning as in (a), we find that the

i^{th} coordinate of $P(fg)\vec{v}$ is $v_{(fg)(i)}$. Similarly, the i^{th} coordinate of $P(g)\vec{v}$ is $v'_i = v_{g(i)}$. Therefore, the i^{th} coordinate of $P(f)(P(g)\vec{v})$ is $v'_{f(i)} = v_{g(f(i))} = v_{(fg)(i)}$. This implies $P(fg)\vec{v} = P(f)P(g)\vec{v}$. Since the v_i were arbitrary real numbers, this implies the theorem. □

Example 49. Let

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

so $f = f^{-1}$, $g = g^{-1}$, $h = fg$. Moreover,

$$P(g) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad P(h) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

A direct matrix calculation verifies that $P(f)P(g) = P(fg) = P(h)$ and $P(h^{-1}) = P(g^{-1}f^{-1}) = P(g^{-1})P(f^{-1}) = P(g)P(f)$, as predicted by the above theorem.

The matrix can be determined from the graph of the function $f : T \to T$ as follows: in the $n \times n$ grid of integral points (x, y), with x and y integers between 1 and n inclusive, fill in all the plotted points with $1's$ and all the unplotted points with $0's$ The resulting $n \times n$ array is the matrix $P(f)$.

Rubik's cubers will often, without knowing it perhaps, use the following lemma to solve their cube:

Lemma 50. *Let $r \in S_n$ denote any permutation and let i, j denote distinct integers belonging to $\{1, 2, ..., n\}$. Let s denote the permutation sending i to j:*

$$(i)s = j.$$

Then $s^r = r^{-1}sr$ is the permutation sending $(i)r$ to $(j)r$:

$$s^r((i)r) = (j)r.$$

More specifically (and this is the specific case which this lemma is most often applied): let $i_1, i_2, ..., i_k$ denote distinct integers belonging to $\{1, 2, ..., n\}$. Let s denote the permutation sending i_j to i_{j+1}:

$$s(i_j) = i_{j+1}, \qquad 1 \le j < k, \qquad s(i_k) = i_1, \qquad s(m) = m, \ \ \forall m \notin \{i_1, ..., i_k\}.$$

Then $s^r = r^{-1}sr$ is the permutation sending $(i_j)r$ to $(i_{j+1})r$:

$$s^r((i_j)r) = (i_{j+1})r, \qquad 1 \le j < k, \qquad s^r((i_k)r) = (i_1)r, \qquad s^r(m) = m, \ \ \forall m \notin \{(i_1)r, ..., (i_k)r\}.$$

In other words, if you have a move s which is a 3-cycle on 3 particular edges, say

$$uf \longmapsto ul \longmapsto ur \longmapsto uf,$$

and another move r which sends these edges somewhere else, say $r = F^2$ so that $r : uf \longmapsto df$ but leaves the other edges alone, then $r^{-1}sr$ is the permutation

$$df \longmapsto ul \longmapsto ur \longmapsto df.$$

Try it!

A proof of this lemma will be given in chapter 8.

3.2 Cycle notation

The most common notation for a permutation is probably the "cycle notation". The symbol

$$(a_1\ a_2\ ...\ a_r) \qquad \text{(some r less than or equal to n)}$$

denotes the permutation f of T which is defined by

$$f(a_1) = a_2,\ f(a_2) = a_3,\ ..., f(a_r) = a_1,$$

and $f(i) = i$, if i is not equal to one of the $a_1, ..., a_r$. Such a permutation is called cyclic. The number r is called the length of the cycle.

We call two such cycles $(a_1\ a_2\ ...\ a_r)$ and $(b_1\ b_2\ ...\ b_t)$ disjoint if the sets $\{a_1, a_2, ..., a_r\}$ and $\{b_1, b_2, ..., b_t\}$ are disjoint.

Lemma 51. *If f and g are disjoint cyclic permutations of T then $fg = gf$.*

proof: This is clear since the permutations f and g of T affect disjoint collections of integers, so the permutations may be performed in either order. □

Lemma 52. *The cyclic permutation $(a_1\ a_2\ ...\ a_r)$ has order r.*

proof: Note $f(a_1) = a_2$, $f^2(a_1) = a_3$, ..., $f^{r-1}(a_1) = a_r$, $f^r(a_1) = a_1$, by definition of f. Likewise, for any $i = 1, ..., r$, we have $f^r(a_i) = a_i$. □

Theorem 53. *Every permutation $f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ is the product of disjoint cyclic permutations. More precisely, if f is a permutation of $\{1, 2, ..., n\}$ (with $n > 1$) then there are non-empty disjoint subsets of distinct integers*

$$S_1 = \{a_{11}, ..., a_{1,r_1}\} \subset \{1, 2, ..., n\},$$
$$S_2 = \{a_{21}, ..., a_{2,r_2}\} \subset \{1, 2, ..., n\},$$
$$...,$$
$$S_k = \{a_{k1}, ..., a_{k,r_k}\},$$

such that

$$\{1, 2, ..., n\} = S_1 \cup ... \cup S_k, \qquad n = r_1 + r_2 + ... + r_k,$$

and

$$f = (a_{11}, ..., a_{1,r_1})...(a_{k1}, ..., a_{k,r_k}).$$

This product is called a cycle decomposition of f . If we rearrange the cardinalities r_i of these sets S_i in decreasing order, say we write this as

$$r'_1 \geq r'_2 \geq ... \geq r'_k,$$

then the k-tuple $(r'_1, ..., r'_k)$ is called the cycle structure of f and f is called a $(r'_1, ..., r'_k)$-cycle. For example, $(1, 2)(3, 4, 5)$ is a $(3, 2)$-cycle.

proof: The proof is constructive.

Let $f : T \to T$ be a permutation. List all the elements

$$\{c_{10} = 1, c_{11} = f(1), c_{12} = f^2(1), c_{13} = f^3(1), ...\},$$

(which must, of course, be finite in number but might also only contain the single element $c_{10} = 1$). This is called the "orbit of 1 under f". Now list the elements in the "orbit of 2":

$$\{c_{20} = 2, c_{21} = f(2), c_{22} = f^2(2), c_{23} = f^3(2), ...\},$$

and so on until we get to the "orbit of n":

$$\{c_{n0} = 2, c_{n1} = f(n), c_{n2} = f^2(n), c_{n3} = f^3(n), ...\}.$$

If you pick any two of these n sets, they will either be the same (up to ordering) or disjoint. Denote all the distinct orbits which contain at least

two elements by $O_1, ..., O_k$. (It doesn't matter what order you write them in or in what order you write the elements in each individual orbit.) Suppose that

$$\begin{aligned} O_1 &= a_{11}, ..., a_{1,r_1} \quad \text{so } |O_1| = r_1, \\ O_2 &= a_{21}, ..., a_{2,r_2} \quad \text{so } |O_2| = r_2, \\ &\vdots \\ O_k &= a_{k1}, ..., a_{k,r_k} \quad \text{so } |O_k| = r_k. \end{aligned}$$

In this case, $r_1 + r_2 + ... + r_k \leq n$, with equality if and only if none of the orbits is a singleton. The cycle notation of f is the expression

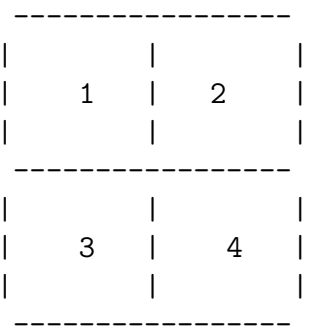
$$(a_{11}a_{12}...a_{1,r1})...(a_{k1}\ a_{k2}\ ...\ a_{k,r_k}).$$

□

Example 54.

- The cycle notation for
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
is (1 2).
- The cycle notation for
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
is (1 2 3).
- The cycle notation for
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
is (1 3)(2 4) = (2 4)(1 3).
- The cycle notation for
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$
is (1 3)(2 4 5) = (4 5 2)(1 3).
- The disjoint cycle decomposition of $(2, 3, 7)(3, 7, 10)$ is $(2, 3)(7, 10)$.

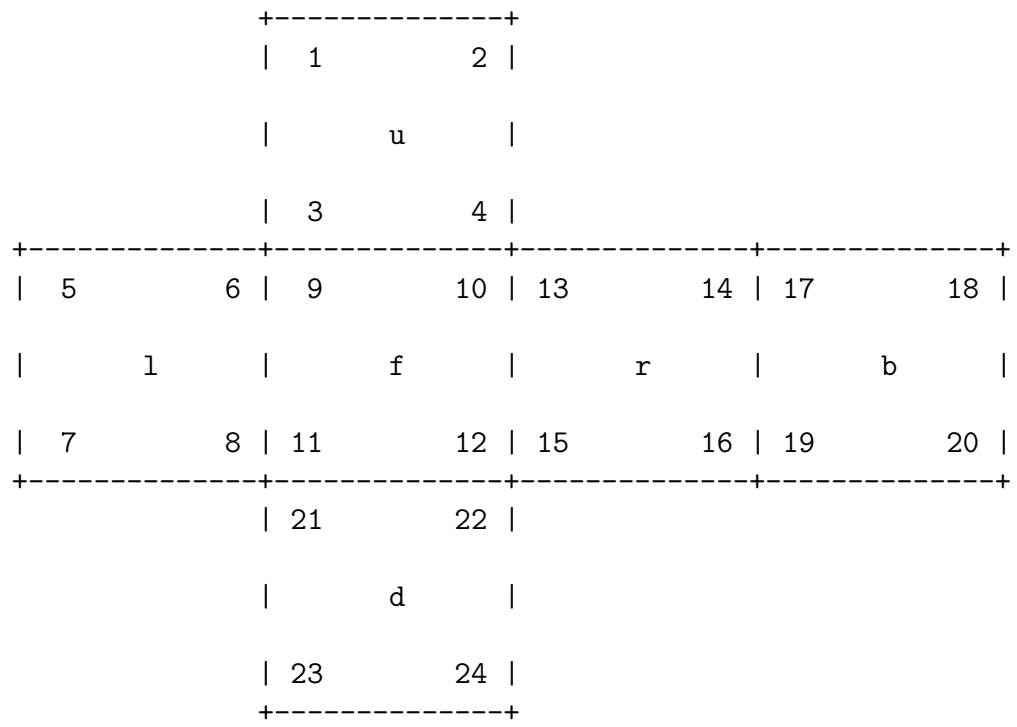
Exercise 3.2.1. Divide a square into 4 subsquares ("facets") and label them $1, 2, 3, 4$. For example,



Let r denote counterclockwise rotation by 90 degrees. Then, as a permutation on the facets, $r = (1\ 3\ 4\ 2)$. Let f_x denote reflection about the horizonal line dividing the square in two, let f_y denote reflection about the vertical line dividing the square in two. Use the cycle notation to determine the permutations of the facets

(a) r^2
(b) r^3,
(c) f_x,
(d) f_y,
(e) $f_x * r * f_x$,
(f) $f_x * f_y$.

Exercise 3.2.2. Label the 24 facets of the 2×2 Rubik's cube as follows:



(You may want to xerox this page then cut this cube out and tape it together for this exercise.) Let X denote rotation clockwise by 90 degrees of the face labeled x, where $x \in \{r, l, f, b, u, d\}$ (so, for example, if $x = f$ then $X = F$). Use the cycle notation to determine the permutations of the facets given by

(a) R,
(b) L,
(c) F,
(d) B,
(e) U,
(f) D.

Lemma 55. *A cyclic permutation is even if and only if the length of its cycle is odd. A general permutation $f : T \to T$ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.*

We shall not prove this here. (For a proof, see Theorem 3.3 in Gaglione [G], §3.2.)

Lemma 56. *The order of a permutation is the least common multiple (lcm) of the lengths $r_1, r_2, ..., r_k$ of the disjoint cycles in its cycle decomposition.*

Example 57. The order of (1 3)(2 4) is 2. It is even. The order of (1 3)(2 4 5) is 6. It is odd.

3.3 An algorithm to list all the permutations

In Martin Gardner's Scientific American article [Gar1] an algorithm is mentioned which lists all the permutations of $\{1, 2, ..., n\}$. This algorithm, due originally to the mathematician Hugo Steinhaus, gives the fastest known method of listing all permutations of $\{1, 2, ..., n\}$.

We shall denote each permutation by the second row in its $2 \times n$ array notation.

For example, in the case $n = 2$:

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$$

are the permutations.

To see the case $n = 3$, the idea is to

(a) write down each row $n = 3$ times each as follows:

$$\begin{matrix} 1 & 2 \\ 1 & 2 \\ 1 & 2 \\ 2 & 1 \\ 2 & 1 \\ 2 & 1 \end{matrix}$$

(b) "weave" in a 3 as follows

$$\begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{matrix}$$

In case $n = 4$, the idea is to

(a) write down each row $n = 4$ times each as follows:

$$
\begin{array}{ccc}
1 & 2 & 3 \\
1 & 2 & 3 \\
1 & 2 & 3 \\
1 & 2 & 3 \\
1 & 3 & 2 \\
1 & 3 & 2 \\
1 & 3 & 2 \\
1 & 3 & 2 \\
3 & 1 & 2 \\
3 & 1 & 2 \\
3 & 1 & 2 \\
3 & 1 & 2 \\
3 & 2 & 1 \\
3 & 2 & 1 \\
3 & 2 & 1 \\
3 & 2 & 1 \\
2 & 3 & 1 \\
2 & 3 & 1 \\
2 & 3 & 1 \\
2 & 3 & 1 \\
2 & 1 & 3 \\
2 & 1 & 3 \\
2 & 1 & 3 \\
2 & 1 & 3
\end{array}
$$

(b) now "weave" a 4 in:

1	2	3	4
1	2	4	3
1	4	2	3
4	1	2	3
4	1	3	2
1	4	3	2
1	3	4	2
1	3	2	4
3	1	2	4
3	1	4	2
3	4	1	2
4	3	1	2
4	3	2	1
3	4	2	1
3	2	4	1
3	2	1	4
2	3	1	4
2	3	4	1
2	4	3	1
4	2	3	1
4	2	1	3
2	4	1	3
2	1	4	3
2	1	3	4

In general, we have the following

Theorem 58. *(Steinhaus) There is a sequence of (not necessarily distinct) 2-cycles,* (a_1, b_1),...,(a_N, b_N), *where* $N = n! - 1$, *such that each non-trivial permutation* f *of* $\{1, 2, ..., n\}$ *may be expressed in the form*

$$f = \prod_{i=1}^{k} (a_i, b_i),$$

for some k, $1 \leq k \leq N$. *Furthermore, these products (for* $k = 1, 2, ..., N$*) are all distinct.*

In other words, each permutation may be written as a product of (not necessarily disjoint) 2-cycles. This will be proven in section 5.11 on Campanology below.

There is an analogous result valid only for *even* permutations: each even permutation may be written as a product of (not necessarily disjoint) 3-cycles. This will be stated more precisely (and proved) later — see Proposition 159.

Chapter 4

Permutation Puzzles

> "How can it be that mathematics, being after all a product of human thought independent of experience, is so admirably adapted to the objects of reality?"
> *Albert Einstein*

> "Though this be madness, yet there is method in't."
> *Shakespeare*

We shall describe several permutation puzzles in this chapter.

A one person game is a sequence of moves following certain rules satisfying

- there are finitely many moves at each stage,
- there is a finite sequence of moves which yields a solution,
- there are no chance or random moves,
- there is complete information about each move,
- each move depends only on the present position, not on the existence or non-existence of a certain previous move (such as chess, where castling is made illegal if the king has been moved previously).

A permutation puzzle is a one person game (solitaire) with the following five properties listed below. Before listing the properties, we define the "puzzle position" to be the set of all possible legal moves. The five properties of a permutation puzzle are:

1. for some $n > 1$ depending only on the puzzle's construction, each move of the puzzle corresponds to a unique permutation of the numbers in $T = \{1, 2, ..., n\}$,

2. if the permutation of T in (1) corresponds to more than one puzzle move then the the two positions reached by those two respective moves must be indistinguishable,

3. each move, say M, must be "invertible" in the sense that there must exist another move, say M^{-1}, which restores the puzzle to the position it was at before M was performed,

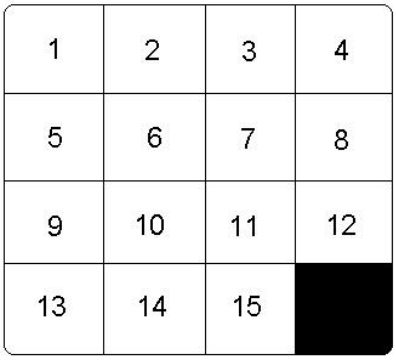
4. if M_1 is a move corresponding to a permutation f_1 of T and if M_2 is a move corresponding to a permutation f_2 of T then $M_1 * M_2$ (the move M_1 followed by the move M_2) is either

   - not a legal move, or
   - corresponds to the permutation $f_1 * f_2$.

Notation: As in step 4 above, we shall always write successive puzzle moves *left-to-right*.

4.1 15 puzzle

One of the earliest and most popular permutation puzzles is the "15 puzzle". The "solved position" looks like

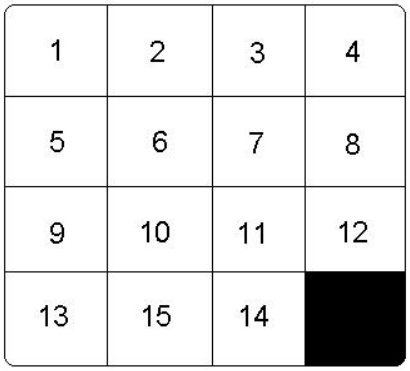


The 15 puzzle

These numbered squared represent sliding blocks which can only move into the blank square. We shall sometimes label the blank square as "16" for convenience. The moves of the puzzle consist of sliding numbered squares (such as 12, for example) into the blank square (e.g., swapping 12 with 16). In this way, each move of this puzzle may be regarded as a permutation of the integers in $\{1, 2, ..., 16\}$.

Exercise 4.1.1. Check that the five conditions of a permutation puzzle are satisfied by the 15 puzzle.

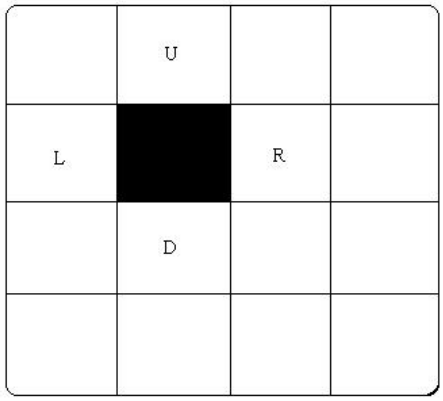
Not every permutation of the $\{1, 2, ..., 16\}$ corresponds to a possible position of the puzzle. For example, the position



The 14-15 puzzle

cannot be attained from the previous position. (The mathematical reason for this is explained in 6.3 below, for example.) Apparently, the puzzle inventor Sam Loyd applied for a U.S. patent for the above puzzle (the one with the 14, 15 swapped) but since it could not be "solved" - i.e., put in the correct order $1, 2, ..., 15$ - no working model could be supplied, so his patent was denied. (This is in spite of the fact that there were apparently thousands of them on the market already.)

The moves of the 15 puzzle may be denoted as follows: suppose we are in a position such as



The 15 puzzle

The possible moves are

$$R = R_{u,r,d,l} = (r\ 16) = \text{ swap r and 16},$$
$$L = L_{u,r,d,l} = (l\ 16) = \text{swap l and 16},$$
$$U = U_{u,r,d,l} = (u\ 16) = \text{swap u and 16},$$
$$D = D_{u,r,d,l} = (d\ 16) = \text{swap d and 16}.$$

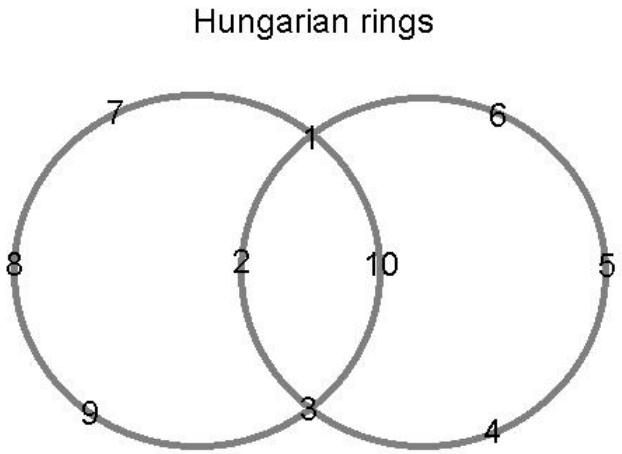
Exercise 4.1.2. Verify that the five defining properties of a permutation puzzle are satisfied by this example.

We shall call the 15 puzzle a planar puzzle since all its pieces lie on a flat board.

4.2 Devil's circles (or Hungarian rings)

This is a planar puzzle consisting of two or more interwoven ovals, each of which has several labeled (by colors or numbers) pieces, some of which may belong to more than one oval. A puzzle move consists of shifting an oval by one or more "increments", and hence all the pieces on it, along the oval's grooved track. The pieces are equally spaced apart (in spite of the typed depiction below) and those pieces which lie on more than one oval can be moved along either oval.

For simplicity, consider the puzzle consisting of only two ovals, each having 6 pieces:



The pieces 1 and 3 can be moved along either oval. Note that each move corresponds to a unique permutation of the numbers in $\{1, 2, ..., 10\}$. For example, rotating the right-hand oval clockwise one increment corresponds to the permutation

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 1 & 2 & 3 & 4 & 5 & 7 & 8 & 9 & 10 \end{array}$$

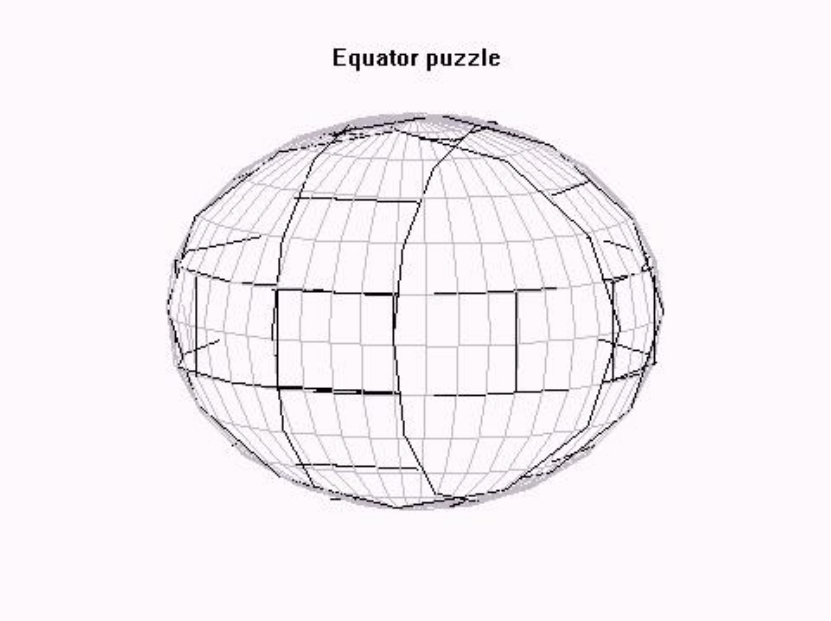
which we may write in cycle notation as (6 5 4 3 2 1).

Exercise 4.2.1. Verify that the five defining properties of a permutation puzzle are satisfied by this example.

4.3 Equator puzzle

This puzzle is in the shape of a sphere but has 3 circular bands encircling a sphere, each having 12 square-shapped pieces and each band intersecting each other at a 90 degree angle. Each pair of circles intersects at two points, or "nodes", and at each such node there is a puzzle piece shared by the two circular bands. There are 6 nodes total. The total number of movable pieces is therefore $3 \cdot 12 - 6 = 30$.

On some puzzles the sphere is painted a map of the earth, others have colored puzzle pieces. The rough idea, minus any colors, is depicted in the following picture:



For concreteness, suppose we are looking at a globe equator puzzle. The longitudinal band circles the equator, one latitudinal band passes through North America and the other latitudinal band passes through Europe and Africa. A move of the puzzle consists of rotating one of the bands (along with all the pieces it contains) in either direction. Successive puzzle moves may change the "orientation" of a piece, as we will see later. When the 30 pieces are such that the puzzle is a correct map of the Earth then we call the position "solved".

For ease of drawing, let us redraw the globe of the Earth using the "Mercatur projection", i.e., as a wall map:

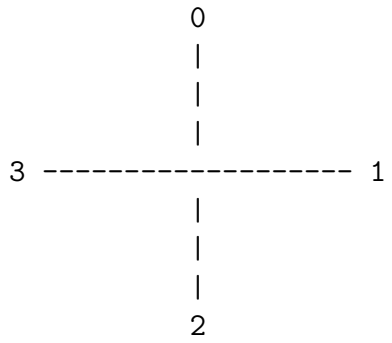
```
1              1              1              1
2             13             12             22
3             14             11             21
4  23  24     15  25  26     10  27  28     20  29  30
5             16              9             19
6             17              8             18
7              7              7              7

          The "solved" position
```

Sometimes we shall also denote 1 by NP ("north pole") and 7 by SP ("south pole").

This description is a little misleading due to the fact that it tells us where a piece is but not, for example, whether it is upside down or not. We shall ignore this problem for now and simply describe how a move affects the position of a piece. We see from the above labeling that any move of the Equator puzzle corresponds to a unique permutation of the integers in 1, 2, ..., 30. For example, the move which rotates the equator east-to-west by 30 degrees corresponds to the permutation

(4 30 29 20 28 27 10 26 25 15 24 23).

Now we shall show to assign an orientation to a piece. We shall regard an orientation (which is, after all, simply an indication of what angle the piece is "twisted") as an integer 0, 1 ,2, or 3. First, if a piece is not in its correct position, it gets an orientation of 0. If a piece is in its correct position then it gets a 0, 1, 2, or 3, depending on its angle from the correct angle (i.e., the angle the piece has in the "solved" position):



Example 59. A piece which has been rotated by 90 degrees counterclockwise from its correct orientation gets an orientation of 3.

In general, the labels for the pieces of the Equator puzzle should be choosen from the set given by the Cartesian product of the set of integers

used to label the positions, $\{1, 2, ..., 30\}$, by the set of integers used to label the orientations:

$$S = \{1, 2, ..., 30\} \times \{0, 1, 2, 3\} = \{(m, n) \mid 1 \leq m \leq 30, 0 \leq n \leq 3\}.$$

Each move of the Equator corresponds to a unique permutation of the set S. There are 120 elements of S, call them

$$S = \{s_1, s_2, ..., s_{120}\}.$$

If we identify the set S with the set $T = \{1, ..., 120\}$ then we move of the Equator corresponds to a unique permutation of the set T.

Exercise 4.3.1. Verify that the Equator puzzle satisfies the five defining properties of a permutation puzzle.

Question: Can you show the following: If a piece is correctly oriented then its antipodal piece is also correctly oriented?

Notation: We introduce notation for 3 basic moves of the Equator puzzle which generate all possible puxzzle moves. Let us label the three circular bands on the globe as C1, C2, and C3. Let C1 be the band which, in the solved position, contains the pieces labeled 1, 2, ..., 12; let C2 be the band which, in the solved position, contains the pieces labeled 7, 13, ..., 22; and let C3 be the band which, in the solved position, contains the pieces on the equator.

Let r_1 be the puzzle move associated to the rotation of C1 given by

$$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 \end{array}$$

Let r_2 be the puzzle move associated to the rotation of C2 given by

$$\begin{array}{cccccccccccc} 1 & 13 & 14 & 15 & 16 & 17 & 17 & 18 & 19 & 20 & 21 & 22 \\ 13 & 14 & 15 & 16 & 17 & 17 & 18 & 19 & 20 & 21 & 22 & 1 \end{array}$$

Let r_3 be the puzzle move associated to the rotation of C3 given by

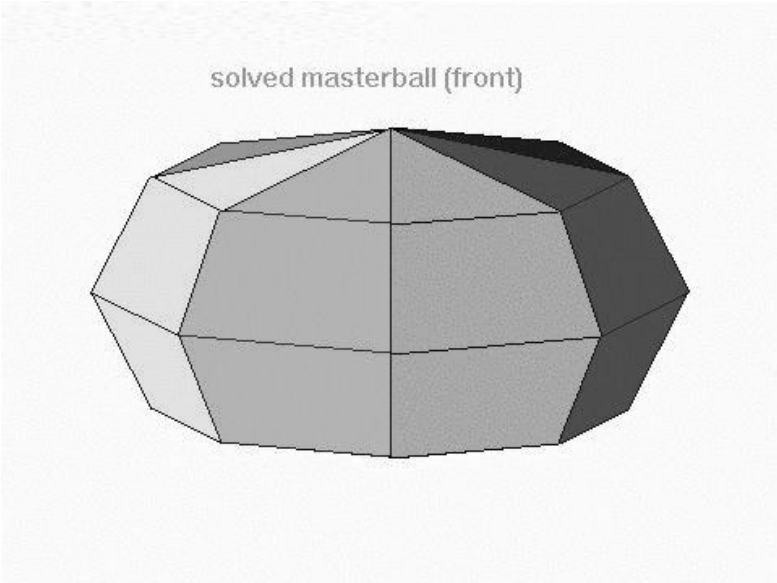
$$\begin{array}{cccccccccccc} 4 & 23 & 24 & 15 & 25 & 26 & 10 & 27 & 28 & 20 & 29 & 30 \\ 30 & 4 & 23 & 24 & 15 & 25 & 26 & 10 & 27 & 28 & 20 & 29 \end{array}$$

It is clear after a little thought that each of these moves corresponds to a permutation of the 120 position/orientation labels of the pieces of the equator puzzle. Furthermore, such a permutation determines the puzzle position uniquely since it specifies the facet's position and orientation.

Exercise 4.3.2. Verify that the remaining properties of a permutation puzzle are satisfied.

4.4 Rainbow Masterball

Some rules for the rainbow masterball (referred to simply as "masterball" in the following): A masterball sphere has 32 tiles of 8 distinct colors. We shall assume that the masterball is in a fixed position in space, centered at the origin. A geodesic path from the north pole to the south pole is called a longitudinal line and a closed geodesic path parallel to the equator is called a latitudinal line. There are 8 longitudinal lines and 3 latitudinal lines. In spherical coordinates, the longitudinal lines are at the angles which are multiples of $\pi/4$ (i.e., at $\theta = n\pi/4,\ n = 1, .., 8$) and the latitudinal lines are at $\phi = \pi/4, \pi/2, 3\pi/4$. (Here $\pi = 3.141592...$ as usual.)



The sphere shall be oriented by the right-hand rule - the thumb of the right hand wrapping along the polar axis points towards the north pole. We assume that one of the longitudinal lines has been fixed once and for all. This fixed line shall be labeled "1", the next line (with respect to the orientation above) as "2", and so on.

Allowed moves: One may rotate the masterball east-to-west by multiples of $\pi/4$ along each of the 4 latitudinal bands or by multiples of π along each of the 8 longitudinal lines.

A facet will be one of the 32 subdivisions of the masterball created by these geodesics. A facet shall be regarded as immobile positions on the sphere

and labeled either by an integer $i \in \{1, ..., 32\}$ or by a pair $(i, j) \in [1, 4] \times [1, 8]$, whichever is more convenient at the time. If a facet has either the north pole or the south pole as a vertex then we call it a small (or polar) facet. Otherwise, we call a facet large (or middle or equatorial). A coloring of the masterball will be a labeling of each facet by one of the 8 colors in such a way that

(a) each of the 8 colors occurs exactly twice in the set of the 16 small facets,

(b) each of the 8 colors occurs exactly twice in the set of the 16 large facets.

A move of the masterball will be a change in the coloring of the masterball associated to a sequence of manuevers as described above.

If we now identify each of the 8 colors with an integer in $\{1, ..., 8\}$ and identify the collection of facets of the masterball with a 4×8 array of integers in this range. To solve an array one must, by an appropriate sequence of moves corresponding to the above described rotations of the masterball, put this array into a "rainbow" position so that the matrix entries of each column has the same number. Thus the array

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array}$$

is "solved". The array

$$\begin{array}{cccccccc} 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array}$$

corresponds to a rotation of the north pole facets by $3\pi/4$.

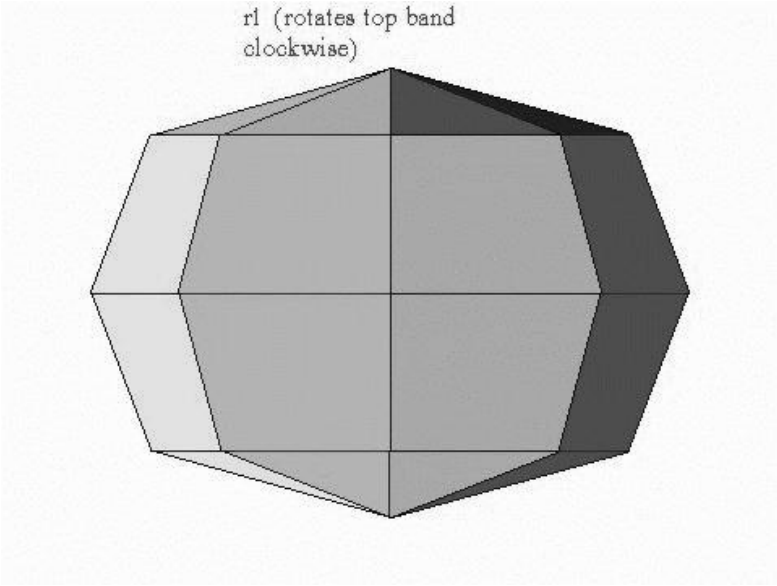
Notation We use matrix notation to denote the 32 facets of the masterball. The generators for the latitudinal rotations are denoted r_1, r_2, r_3, r_4. For example, r_1 sends

$$\begin{array}{cccccccc} 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \end{array}$$

to

12	13	14	15	16	17	18	11
21	22	23	24	25	26	27	28
31	32	33	34	35	36	37	38
41	42	43	44	45	46	47	48

which is pictured as:



As you look down at the ball from the north pole, this move rotates the ball clockwise. The other moves r_2, r_3, r_4 rotate the associated band of the ball in the same direction - clockwise as viewed from the north pole.

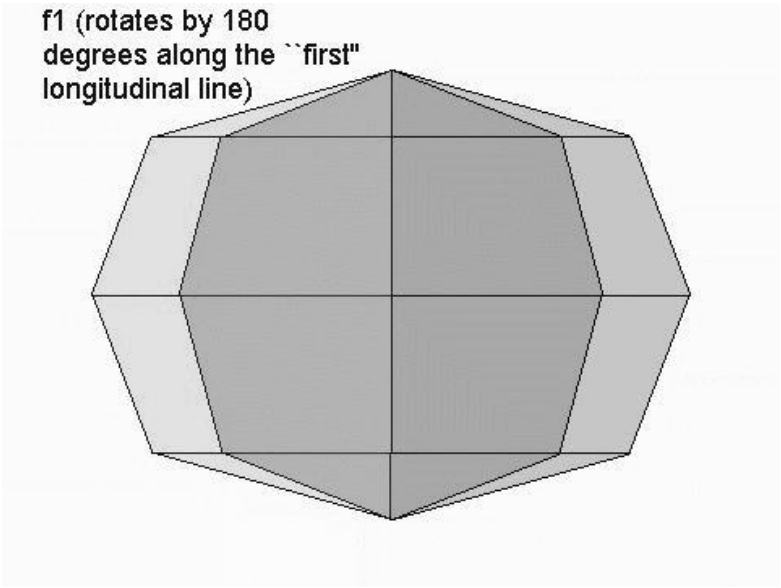
The generators for the longitudinal rotations are denoted $f_1, f_2, ..., f_8$. For example, f_1 sends

11	12	13	14	15	16	17	18
21	22	23	24	25	26	27	28
31	32	33	34	35	36	37	38
41	42	43	44	45	46	47	48

to

44	43	42	41	16	17	18	11
34	33	32	31	25	26	27	28
24	23	22	21	35	36	37	38
15	14	13	12	45	46	47	48

which is pictured as:



With these rules, one can check the relation

$$f_5 = r_1^4 * r_2^4 * r_3^4 * r_4^4 * f_1 * r_1^4 * r_2^4 * r_3^4 * r_4^4.$$

Exercise 4.4.1. Find similar identities for f_6, f_7, f_8.

Also, one can check that

$$r_1 = (f_3 * f_7)^{-1} * r_4^{-1} * f_3 * f_7.$$

Exercise 4.4.2. There are similar identities for r_2, r_3, r_4. Find them.

Identify the facets of the masterball with the entries of the array

8	7	6	5	4	3	2	1
16	15	14	13	12	11	10	9
24	23	22	21	20	19	18	17
32	31	30	29	28	27	26	25

(there is a reason for labeling the facets "backwards" like this but it's not important). We may express the generators of the masterball group in disjoint

cycle notation as a subgroup of S_{32} (the symmetric group on 32 letters):

$$\begin{aligned}
r_1^{-1} &= (1\,2\,3\,4\,5\,6\,7\,8),\\
r_2^{-1} &= (9\,10\,11\,12\,13\,14\,15\,16),\\
r_3^{-1} &= (17\,18\,19\,20\,21\,22\,23\,24),\\
r_4^{-1} &= (25\,26\,27\,28\,29\,30\,31\,32),\\
f_1 &= (5\,32)(6\,31)(7\,30)(8\,29)(13\,24)(14\,23)(15\,22)(16\,21),\\
f_2 &= (4\,31)(5\,30)(6\,29)(7\,28)(12\,23)(13\,22)(14\,21)(15\,20),\\
f_3 &= (3\,30)(4\,29)(5\,28)(6\,27)(11\,22)(12\,21)(13\,20)(14\,19),\\
f_4 &= (2\,29)(3\,28)(4\,27)(5\,26)(10\,21)(11\,22)(12\,23)(13\,24),\\
f_5 &= (1\,28)(2\,27)(3\,26)(4\,25)(9\,20)(10\,19)(11\,18)(12\,17),\\
f_6 &= (8\,27)(1\,26)(2\,25)(3\,32)(16\,19)(9\,18)(10\,17)(11\,24),\\
f_7 &= (7\,26)(8\,25)(1\,32)(2\,31)(15\,18)(16\,17)(9\,24)(10\,23),\\
f_8 &= (6\,25)(7\,32)(8\,31)(1\,30)(14\,17)(15\,24)(16\,23)(9\,22),
\end{aligned}$$

Exercise 4.4.3. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

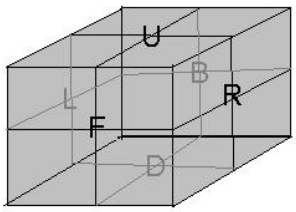
More information on this puzzle will be given in a later chapter.

4.5 Rubik's cubes

We shall introduce the 2×2, 3×3, 4×4, and higher Rubik's cubes.

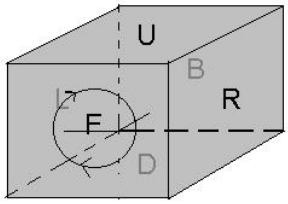
4.5.1 2×2 Rubik's cube

The "pocket" Rubik's cube has 6 sides, or "faces", each of which has $2 \cdot 2 = 4$ "facets", for a total of 24 facets:



6 sides: (F) front, B (back),
L (left), R (right), U (up), D (down)

Fix an orientation of the Rubik's cube in space. Therefore, we may label the 6 sides as f, b, l, r, u, d, as in the picture. It has 8 subcubes. Each face of the cube is associated to a "slice" of 4 subcubes which share a facet with the face. The face, along with all of the 4 cubes in the "slice", can be rotated by 90 degrees clockwise. We denote this move by the upper case letter associated to the lower case letter denoting the face. For example, F denotes the move which rotates the front face by 90 degrees to clockwise.



The move F

As in chapter 4, we label the 24 facets of the 2×2 Rubik's cube as follows:

```
                +--------------+
                |  1         2 |
                |       u      |
                |  3         4 |
+---------------+--------------+--------------+--------------+
|  5         6 |  9        10 | 13        14 | 17        18 |
|       l       |       f      |       r      |       b      |
|  7         8 | 11        12 | 15        16 | 19        20 |
+---------------+--------------+--------------+--------------+
                | 21        22 |
                |       d      |
                | 23        24 |
                +--------------+
```

The 24 facets will be denoted by xyz where x is the face on which the facet lives and y, z (or z, y - it doesn't matter) indicate the 2 edges of the facet. Written in clockwise order:

```
front face:  fru, frd, fld, flu
 back face:  blu, bld, brd, bru
right face:  rbu, rbd, rfd, rfu
 left face:  lfu, lfd, lbd, lbu
   up face:  urb, urf, ulf, ulb
 down face:  drf, drb, dlb, dlf
```

Exercise 4.5.1. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

For future reference, we call this system of notation (which we will also use for the 3×3 and 4×4 Rubik's cube) the Singmaster notation.

4.5.2 3×3 Rubik's cube

In this section we shall, for the most part, simply introduce enough notation (due to Singmaster [Si]) to allow us to check that the puzzle is in fact a permutation puzzle. We shall also introduce a two-person game which is easier to play and learn than solving the cube.

The Rubik's cube has 6 sides, or "faces", each of which has $3 \cdot 3 = 9$ "facets", for a total of 54 facets. We label these facets $1, 2, ..., 54$ as follows:

```
                +--------------+
                |  1    2    3 |
                |  4    u    5 |
                |  6    7    8 |
+---------------+--------------+--------------+--------------+
|  9   10   11 | 17   18   19 | 25   26   27 | 33   34   35 |
| 12    l   13 | 20    f   21 | 28    r   29 | 36    b   37 |
| 14   15   16 | 22   23   24 | 30   31   32 | 38   39   40 |
+---------------+--------------+--------------+--------------+
                | 41   42   43 |
                | 44    d   45 |
                | 46   47   48 |
                +--------------+
```

then the generators, corresponding to the six faces of the cube, may be written in disjoint cycle notation as:

$$F = (17\,19\,24\,22)(18\,21\,23\,20)(6\,25\,43\,16)(7\,28\,42\,13)(8\,30\,41\,11),$$
$$B = (33\,35\,40\,38)(34\,37\,39\,36)(3\,9\,46\,32)(2\,12\,47\,29)(1\,14\,48\,27),$$
$$L = (9\,11\,16\,14)(10\,13\,15\,12)(1\,17\,41\,40)(4\,20\,44\,37)(6\,22\,46\,35),$$
$$R = (25\,27\,32\,30)(26\,29\,31\,28)(3\,38\,43\,19)(5\,36\,45\,21)(8\,33\,48\,24),$$
$$U = (1\,3\,8\,6)(2\,5\,7\,4)(9\,33\,25\,17)(10\,34\,26\,18)(11\,35\,27\,19),$$
$$D = (41\,43\,48\,46)(42\,45\,47\,44)(14\,22\,30\,38)(15\,23\,31\,39)(16\,24\,32\,40).$$

Exercise 4.5.2. Check this. (It is helpful to xerox the above diagram, cut it out and tape together a paper cube for this exercise.)

The notation for the facets will be similar to the notation used for the 2×2 Rubik's cube. The corner factes will have the same notation and the edge facets will bve denoted by xy, where x is the face the facet lives on and y is the face the facet borders to. In clockwise order, starting with the upper right-hand corner of each face:

```
front face:  fru, fr, frd, fd, fld, fl, flu, fu
 back face:  blu, bl, bld, bd, brd, br, bru, bu
right face:  rbu, rb, rbd, rd, rfd, rf, rfu, ru
 left face:  lfu, lf, lfd, ld, lbd, lb, lbu. lu
   up face:  urb, ur, urf, uf, ulf, ul, ulb, ub
 down face:  drf, dr, drb, db, dlb, dl, dlf, df
```

Exercise 4.5.3. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

First fundamental theorem of cube theory

We shall frequently need the following fact:

Theorem 60. *Beginning with a solved cube, label the following facets with an invisible "+" (i.e., mark the spatial position of the facet on the cube with a "+"):*

- *U facet of the uf edge subcube*
- *U facet of the ur edge subcube*
- *F facet of the fr edge subcube*

- *all facets which can be obtained from these by a move of the slice group.*

Label the U and D facets of each corner subcube with an invisible "+". These "+" signs are called the standard reference markings. Each move g of the Rubik's cube yields a new collection of "+" labels, called the markings relative to g. A position of the Rubik's cube is determined by the following decision process:

(a) How are the edge subcubes permuted?

(b) How are the center subcubes permuted?

(c) How are the corner subcubes permuted?

(d) Which of the relative edge markings are flipped (relative to the standard reference markings)?

(e) Which of the relative corner markings are rotated from the standard reference markings and, if so, by how much ($2\pi/3$ or $4\pi/3$ radians clockwise, relative to the standard reference markings)?

This is labeled as a theorem because of its relative importance for us, not because of it's difficulty! This is the "First Fundamental Theorem of Rubik's cube theory".

As an exercise, the reader should convince him or herself that this theorem is correct.

The superflip game

The position of the Rubik's cube where every edge is flipped, but all the others subcubes are unaffected, is called the superflip position.

To play the game, first choose two particular faces as your up (U) and front (F) face - say white is up and red is front (assuming you have a cube with adjacent white and red faces). Imagine the cube being placed in space with rectangular coordinate axes in such a way that the *bdl* corner is at the origin $(0, 0, 0)$, the *dl* edge is along the x-axis and the *bl* edge is along the z-axis.

The rules ("slice-superflip game"):

1. Players alternate making moves starting with the cube in the solved position. The first player is determined by (say) a coin toss.

2. A move consists of flipping over exactly two edges. Both edges must lie in a slice. The edge closest to the origin (or, if this is a tie, closest to the x-axis) must be flipped from "solved" to "wrong".

3. The first player to reach the superflip position wins.

Of course, to play this game you must know several edge-flipping moves, such as those in §14.2.1 below.

This game is related to a game which might be called a "three dimensional acrostic twins game". (See [BCG], vol II, page 441, for a two dimensional acrostic twins game.)

Several alternate versions of this game may also be played.

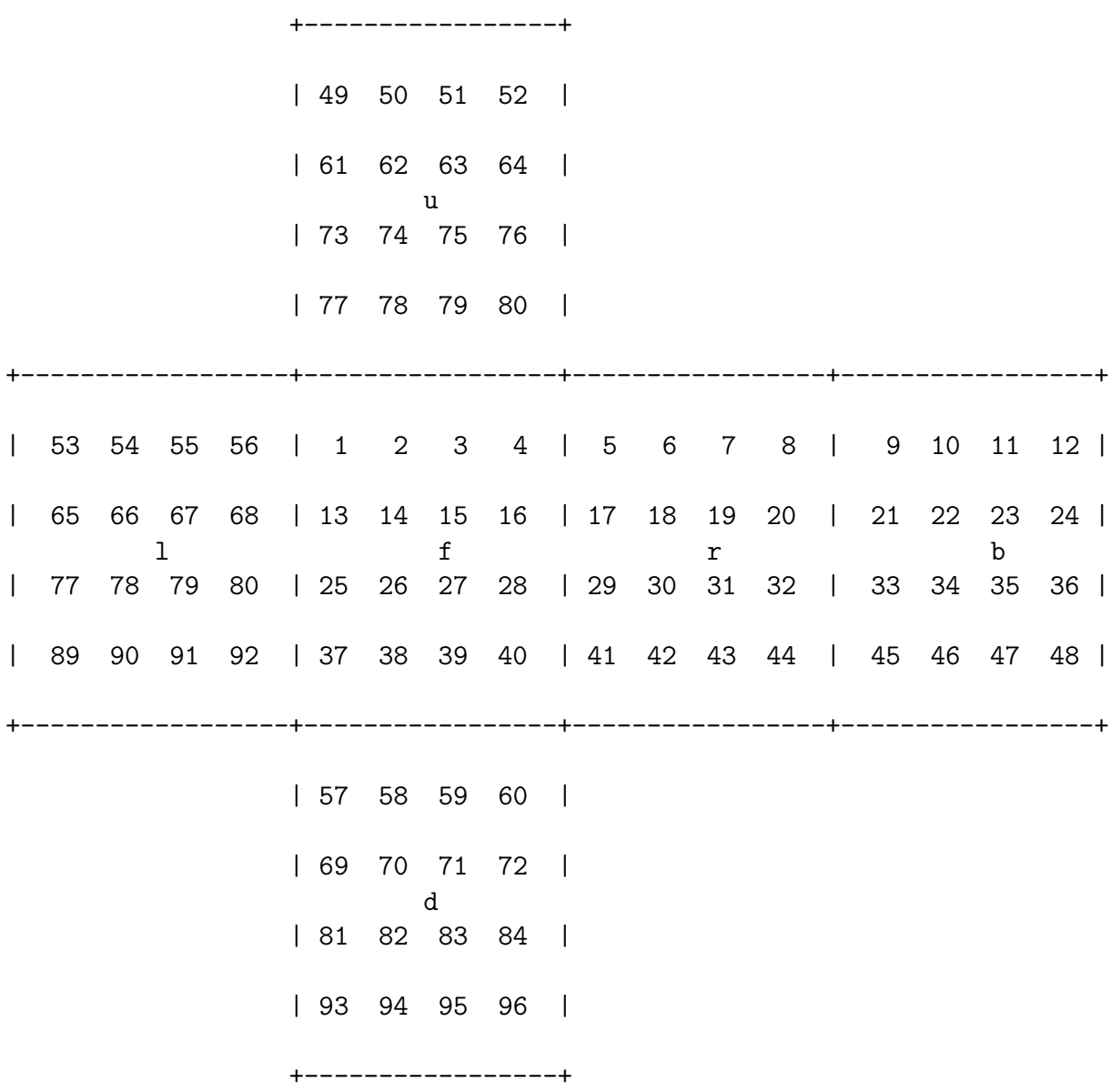
"Nonslice-superflip game": The rules are the same except the condition that the two edges belong to the same slice is either dropped altogether or replaced by the condition that the two edges do not belong to the same slice.

"Möbius-superflip game": The rules for this version are the same except the condition that two edges are flipped is to be replaced by any number of edges less than 6 (i.e., exactly 2, 4, or 6) is to be flipped. This game is related to a game which might be called a "three dimensional Möbius". (See [BCG], vol II, page 434, for a Möbius game.)

Exercise 4.5.4. Play a game!

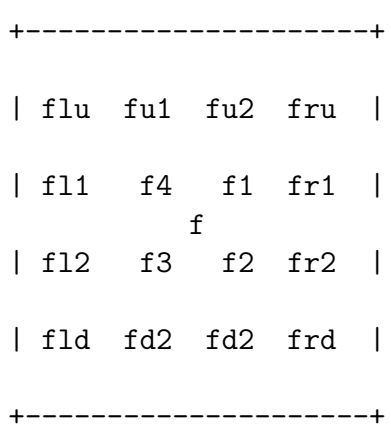
4.5.3 4×4 Rubik's cube

The 4×4 Rubik's cube has 6 sides, or "faces", each of which has $4 \cdot 4 = 16$ "facets", for a total of 96 facets. As usual, we fix an orientation of the cube in space, so we may pick a front face, back face, ... We label these facets $1, 2, ..., 96$ as follows:



The reader may want to xerox the above diagram, cut it out and tape together a paper cube.

Notation: We need notation for the facets and for the moves.
Facets: To label the facets, we must pick an orientation of each face, say clockwise. For example, the the front face may be labeled as



The labeling of the other faces is similar.

Exercise 4.5.5. Label the other 5 faces.

Moves: Parallel to each face x are 4 slices of 16 subcubes each labeled X_1, X_2, X_3, X_4, in order of their distance from the face. For example, the front face f has 16 subcubes comprising the F_1 slice, the two inner slices are F_2, F_3, and the last slice F_4 is actually the same as the first slice B_1 associated to the back face.

The 12 generators (written in disjoint cycle notation), corresponding 2 each to the six faces of the cube are given by:

$$\begin{aligned}
U_1 &= (49\,52\,88\,85)(62\,63\,75\,74)(50\,64\,87\,73)\times \\
&\times(51\,76\,86\,61)(5\,1\,53\,9)(6\,2\,54\,10)(7\,3\,55\,11)(8\,4\,56\,12),\\
U_2 &= (17\,13\,65\,21)(18\,14\,66\,22)(19\,15\,67\,23)(20\,16\,68\,24),\\
L_1 &= (96\,48\,49\,1)(84\,36\,61\,13)(72\,24\,73\,25)(60\,12\,85\,37)\times \\
&\times(89\,53\,56\,92)(90\,65\,55\,80)(91\,77\,54\,68)(66\,67\,79\,78),\\
L_2 &= (59\,11\,86\,38)(71\,23\,74\,26)(83\,35\,62\,14)(95\,47\,50\,2),\\
F_1 &= (89\,5\,93\,92)(77\,17\,81\,80)(65\,29\,69\,68)(53\,41\,57\,86)\times \\
&\times(1\,4\,40\,37)(2\,16\,39\,25)(3\,28\,38\,13)(14\,15\,27\,26),\\
F_2 &= (73\,6\,81\,91)(74\,18\,82\,79)(75\,30\,83\,67)(76\,42\,84\,55),\\
R_1 &= (40\,88\,9\,57)(28\,76\,21\,69)(16\,64\,33\,81)(4\,52\,49\,93)\times \\
&\times(41\,5\,8\,44)(42\,17\,7\,32)(43\,29\,6\,20)(18\,19\,31\,30),\\
R_2 &= (39\,87\,10\,58)(27\,75\,22\,70)(15\,63\,34\,82)(3\,51\,46\,94),\\
B_1 &= (52\,53\,44\,60)(51\,65\,32\,59)(50\,77\,20\,58)(49\,89\,8\,57)\times \\
&\times(9\,12\,48\,45)(10\,24\,47\,33)(11\,36\,46\,21)(22\,23\,35\,34),\\
B_2 &= (54\,72\,43\,64)(66\,71\,31\,63)(78\,70\,19\,62)(90\,69\,7\,61),\\
D_1 &= (57\,60\,96\,93)(58\,72\,95\,81)(59\,84\,94\,69)\times \\
&\times(70\,71\,83\,82)(45\,89\,37\,41)(46\,90\,38\,42)(47\,91\,39\,43)(48\,92\,40\,44),\\
D_2 &= (33\,77\,25\,29)(34\,78\,26\,30)(35\,79\,27\,31)(36\,80\,28\,32).
\end{aligned}$$

Exercise 4.5.6. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

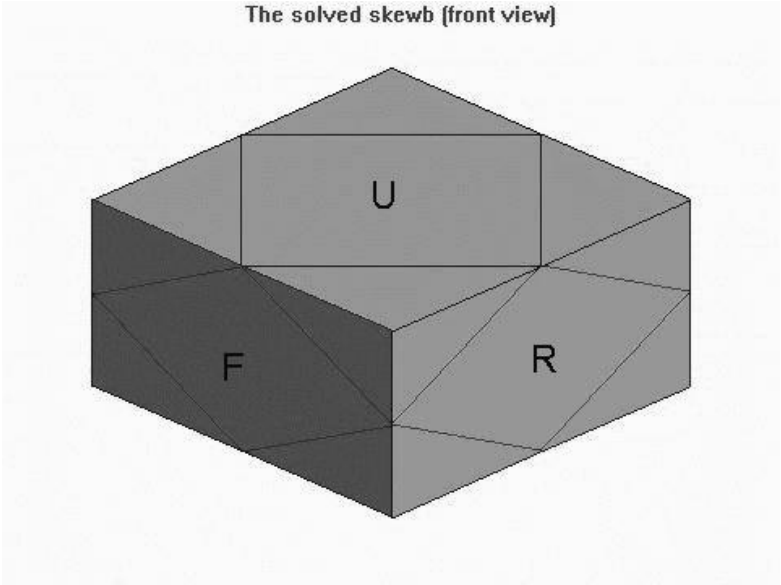
4.5.4 $n \times n$ Rubik's cube

Other than the 2×2, 3×3, and 4×4 cubes, the only other Rubik's cube manufactured, as far as I know, is the 5×5 Rubik's cube. Apparently, there are mechanical problems which cause the manufacture of the $n \times n$ cubes to be overly expensive or perhaps even impossible, for n large. For information, at least theoretically, on the solution of such cubes, the reader might be interested in the article [L] or the postings in the archives of the "cube-lovers" list [CL].

4.6 Skewb

The skewb is a cube which has been subdivided into regions differently than the Rubik's cube. First, fix an orientation of the cube in space, so we may

talk about a front face, a back face, up, down, left, and right. Each of these 6 square faces are subdivided into 5 facets as follows:

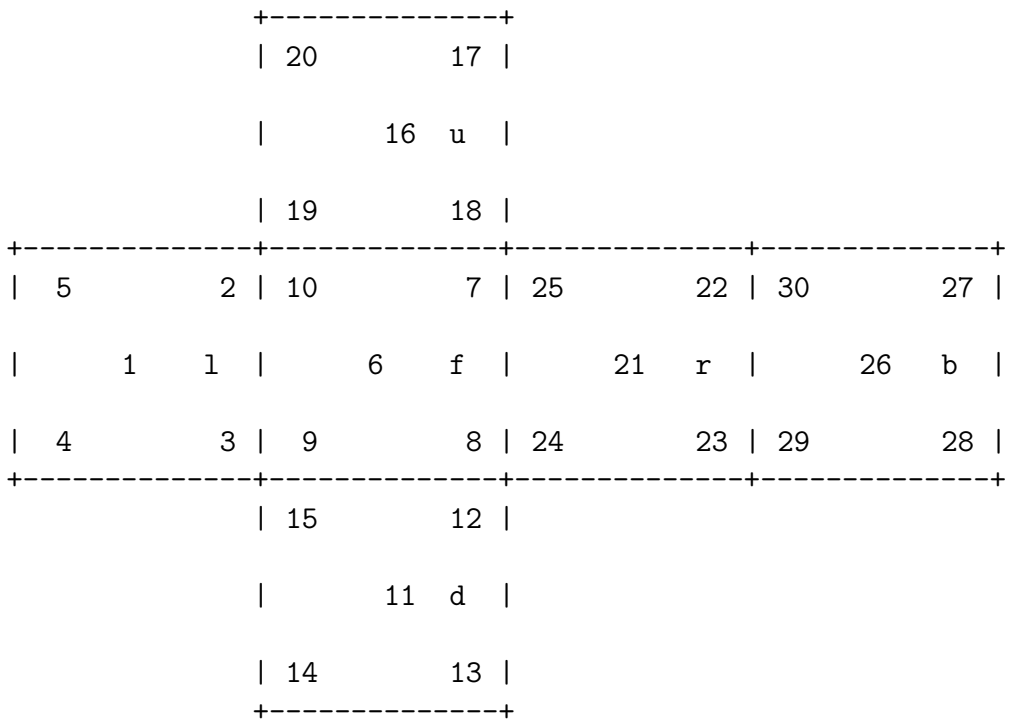


The 4 corner facets are labeled exactly as in the case of the Rubik's cube (as the lower case xyz, where x is the label of the face the facet lives on, y and z the two neighboring faces).

The skewb itself is a cube subdivided as follows: there are 8 corner pieces which are each in the shape of a tetrahedron. For example, if you hold a cube in front of you the upper right hand corner of the front face is the facet of a tetrahedron whose facets are labels f_1, r_4, u_2.

The moves of the skewb are different from the Rubik's cube as well: Label the corners as XYZ, where xyz is the notation for any of the facets belonging to that corner piece. Pick a corner XYZ of the cube and draw a line L passing through that corner vertex and the opposite corner vertex ("skewering the cube"). That line defines a 120 degree rotation in the clockwise direction (viewed from the line looking down onto the corner you picked). One move of the skewb is defined in terms of this rotation as follows: Of course a 120 degree rotation of the entire cube about the line L will preserve the cube but swap some faces and some vertices. The skewb has a mechanism so that you can actually rotate half (a "skewed" half) the skewb by 120 degrees about L and leave the other half completely fixed. This rotation of half the skewb about L will also be denoted XYZ.

We may also label the $5 \cdot 6 = 30$ facets as follows:



Example 61. Consider the rotation UFR associated to the corner ufr. This move permutes the facets of the skewb. As a permutation, the disjoint cycle notation for this move is

$$UFR = (6\ 16\ 21)(7\ 18\ 25)(10\ 17\ 24)(8\ 19\ 22).$$

Note, in particular UFR does not move the 9-facet.

The eight basic moves are given by

$$\begin{aligned}
FUR &= (6\ 16\ 21)(7\ 18\ 25)(10\ 17\ 24)(8\ 19\ 22)\\
RUB &= (21\ 16\ 26)(22\ 17\ 30)(25\ 20\ 29)(23\ 18\ 27)\\
BUL &= (26\ 16\ 1)(27\ 20\ 5)(28\ 17\ 2)(30\ 19\ 4)\\
LUF &= (1\ 16\ 6)(2\ 19\ 10)(5\ 18\ 9)(3\ 20\ 7)\\
FDR &= (11\ 6\ 21)(25\ 13\ 9)(23\ 15\ 7)(24\ 12\ 8)\\
BDR &= (26\ 11\ 21)(29\ 13\ 23)(27\ 12\ 22)(30\ 14\ 24)\\
FDL &= (6\ 11\ 1)(9\ 15\ 3)(10\ 12\ 4)(8\ 14\ 2)\\
LDB &= (1\ 11\ 26)(3\ 13\ 27)(4\ 14\ 28)(5\ 15\ 29).
\end{aligned}$$

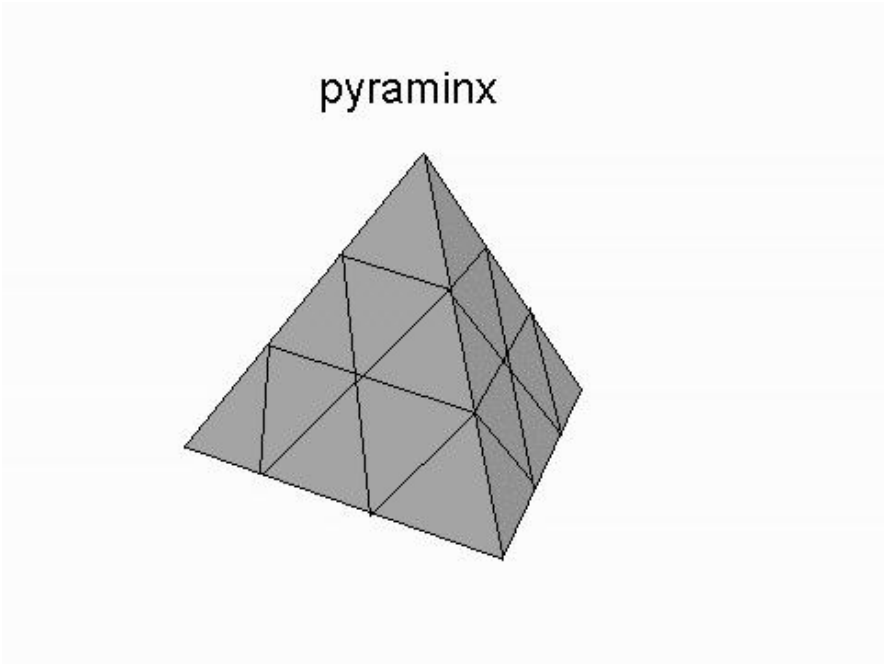
All other moves are obtained by combining these moves sequentially.

The reader who wishes may check these by xeroxing the above diagram, cutting it out and taping it together.

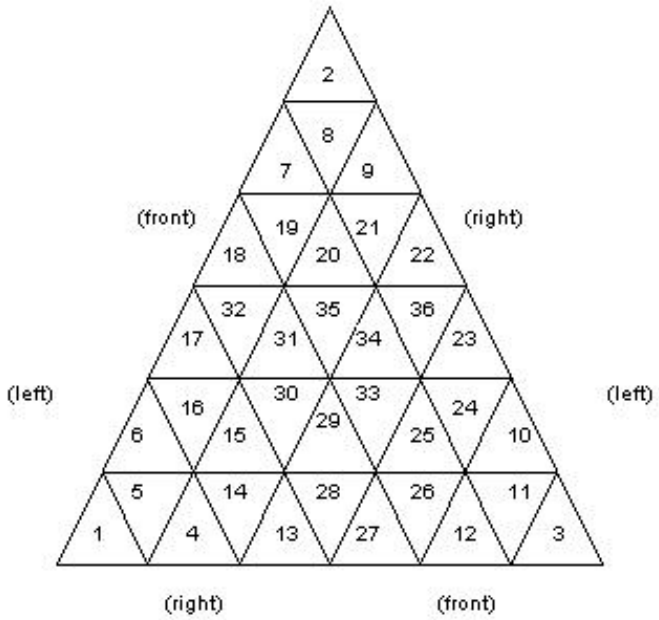
Exercise 4.6.1. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

4.7 Pyraminx

The pyraminx is a puzzle in the shape of a tetrahedron. A tetrahedron is a 4-sided regular platonic solid, all of whose faces are equilateral triangles. Each of the 4 faces of the puzzle is divided into 9 triangular facets:



There are a total of $4 \cdot 9 = 36$ facets on the pyraminx. They will be labeled as follows (the reader may want to xerox this, cut it out, then fold the corners and tape it into a tetrahedron):



We fix an orientation of the tetrahedron in space so that you are looking at a face which we call the "front". We may also speak of a "right", "left", and "down" face. We label the 4 faces as f(ront), r(ight), l(eft), d(own). We label the vertices U(p), R(ight), L(eft), and B(ack).

The tetrahedron itself has been subdivided into sub-tetrahedrons as follows: to each vertex X (so $X \in \{U, R, L, B\}$) there is an opposing face F of the solid. For each such face, we slice the solid along two planes parallel to the vertex X and lying in between the face and the vertex. We want these planes, along with the face and the vertex to be spaced apart equally. The sub-tetrahedrons in the slice of the face itself will be called the face slice associated to the face F, denoted F_1, the sub-tetrahedrons in the middle slice parallel to the face F will be called the middle slice associated to that face, denoted F_2, and the sub-tetrahedron containing the vertex X to the face tip associated to that vertex, denoted F_3.

To each face labeled F, we have a clockwise rotation by 120 degrees of the first slice F_1 of the face. We shall denote this rotation also by F_1. This rotation only moves the facets living on the slice F_1. Similarly, we have a

clockwise rotation by 120 degrees of the second slice F_2 of the face. We shall denote this rotation also by F_2. F_3 denotes the clockwise rotation by 120 degrees of the opposing sub-tetrahedron containing the vertex X. These moves permute the labels for the 36 facets, hence may be regarded as a permutation of the numbers $1, 2, ..., 36$.

For example, the clockwise rotation by 120 degrees (looking at the front face) of the sub-tetrahedron opposite to the front face will be denoted F_3. The disjoint cycle notation for this move, regarded as a permutation, is

$$F3 = (23\ 22\ 36).$$

The basic moves are given as follows:

$$\begin{gathered}
F_1 = (2\ 32\ 27)(8\ 31\ 26)(7\ 30\ 12)(19\ 29\ 11)\times \\
\times(18\ 28\ 3)(1\ 17\ 13)(6\ 15\ 4)(5\ 16\ 14) \\
F_2 = (9\ 35\ 25)(21\ 34\ 24)(20\ 33\ 10) \\
F_3 = (23\ 22\ 36) \\
R_1 = (3\ 36\ 17)(11\ 34\ 16)(10\ 35\ 6)\times \\
\times(24\ 31\ 5)(23\ 32\ 1)(2\ 22\ 18)(9\ 20\ 7)(8\ 21\ 19) \\
R_2 = (12\ 33\ 15)(26\ 29\ 14)(25\ 30\ 4) \\
R_3 = (27\ 28\ 13) \\
L_1 = (1\ 28\ 22)(5\ 29\ 21)(4\ 33\ 9)\times \\
\times(14\ 34\ 8)(13\ 36\ 2)(3\ 27\ 23)(11\ 26\ 24)(12\ 25\ 10) \\
L_2 = (6\ 30\ 20)(16\ 31\ 19)(15\ 35\ 7) \\
L_3 = (17\ 32\ 18) \\
D_1 = (13\ 18\ 23)(14\ 19\ 24)(15\ 20\ 25)\times \\
\times(16\ 21\ 26)(17\ 22\ 27)(28\ 32\ 36)(29\ 31\ 34)(30\ 35\ 33) \\
D_2 = (4\ 7\ 10)(5\ 8\ 11)(6\ 9\ 12) \\
D_3 = (1\ 2\ 3)
\end{gathered}$$

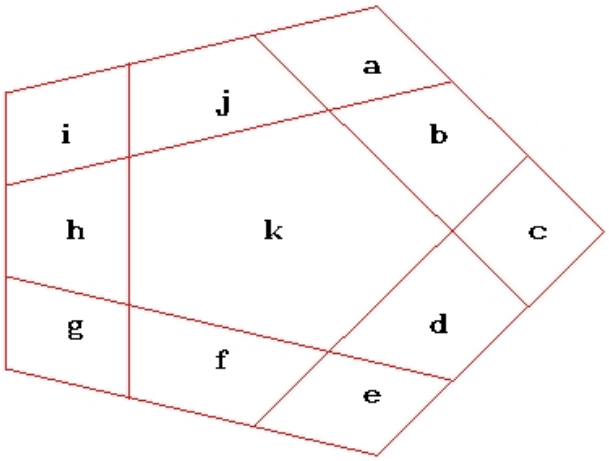
All other moves are obtained by combining these moves sequentially. Indeed, later, we shall want to use moves of the form $F_2 * F_3$, for each face F, but the disjoint cycle notation for these permutations are a little more cumbersome to write down.

Exercise 4.7.1. Verify that the properties of a permutation puzzle are satisfied for this puzzle.

4.8 Megaminx

This puzzle is in the shape of a dodecahedron. A dodecahedron is a 12-sided regular platonic solid for which each of the 12 faces is a pentagon. We call two faces neighboring if they share an edge. There are 20 vertices and 30 edges on a dodecahedron.

Each of the puzzle faces has been subdivided into 11 facets by slicing each edge with a cut which is both parallel to that edge and not far from the edge (say one-fifth the way to the opposite vertex). A picture is as follows:



There are a total of $11 \cdot 12 = 132$ facets on the puzzle. Each face of the solid is parallel to a face on the opposite side. Fix a face of the dodecahedron and consider a plane parallel to that face slicing through the solid and about one-fifth the way to the opposite face. There are 12 such slices. Two such slices associated to two neighboring edges will intersect inside the dodecahedron at a 120 degree angle but two such slices associated to two non-neighboring edges will not intersect inside the dodecahedron (though they will intersect outside the solid of course). We slice up the solid dodecahedron in this way. This creates a smaller dodecahedron in the center and several other irregular smaller pieces.

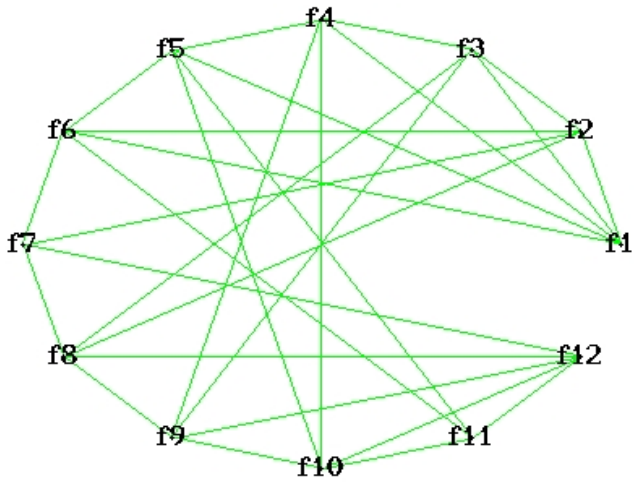
For each such slice associated to a given face f_i there is a basic move still denoted f_i of the megaminx given by clockwise rotating the slice of the

megaminx by 120 degree, leaving the rest of the dodecahedron invariant. Such a move effects 26 facets of the megaminx and leaves the remaining 106 facets completely fixed.

Label the 12 faces of the solid as $f_1, f_2, ..., f_{12}$ in some fixed way. Imagine that the dodecahedron is placed in 3-space in such a way that one side on the xy-plane and is centered along the positive z-axis so that one of the vertices of the top face is at the xyz-coordinate $(r, 0, s)$, where r is the radius of the inscribed circle for the pentagon and s is the distance from the "up" face to the "down" face of the dodecahedron.

Exercise 4.8.1. Suppose $r = 1$. Find s. (This is fairly hard - see the chapter on Platonic solids for some ideas.)

The up face we label as f_1. The others may be labeled according to the following graph, where faces are represented by vertices and two vertices are connected by an edge if the corresponding faces are neighboring.



A more symmetric way to order the faces of the dodecahedron is as follows (see [B], exercise 18.35):

f_1	u
f_2	u_0
f_3	u_1
f_4	u_2
f_5	u_3
f_6	u_4
f_7	d_2
f_8	d_3
f_9	d_4
f_{12}	d
f_{11}	d_1
f_{10}	d_0

One property of this labeling is explained in the following

Exercise 4.8.2. Suppose that the permutation (0 1 2 3 4) of the numbers $\{0, 1, 2, 3, 4\}$ acts on the labels $u_0, ..., u_4$ and $d_0, ..., d_4$ in the obvious way. Show that this permutation of the faces corresponds to a rotation of the dodecahedron.

Notice that, like the cube, each vertex is uniquely determined by specifying the three faces it has in common. We use the notation $x.y.z$ for the vertex of the dodecahedron which lies on the three faces x, y, z. Note that the order is irrelevent: $x.y.z$ denotes the same vertex as $y.x.z$ or $z.y.x$.

The facets of the megaminx may be specified as with the Rubik's cube: a corner facet may be specified as $[x.y.z]$, where x is the face the facet lives on and y, z are the two neighboring faces of the facet. An edge facet may be specified by $[x.y]$, where x is the face the facet lives on and y is the other neighboring face of the facet. The center facet of f_1 will simply be denoted by $[f_1]$. We will call this label the intrinsic label.

We may label the facets of the up face f_1 as follows:

f_1 facet symbol	numerical label	intrinsic label
a	1	$[f_1.f_6.f_2]$
b	2	$[f_1.f_2]$
c	3	$[f_1.f_2.f_3]$
d	4	$[f_1.f_3]$
e	5	$[f_1.f_3.f_4]$
f	6	$[f_1.f_4]$
g	7	$[f_1.f_4.f_5]$
h	8	$[f_1.f_5]$
i	9	$[f_1.f_5.f_6]$
j	10	$[f_1.f_6]$
k	11	$[f_1]$

For the next face (the f_2 face), we label the facets in such a way that the *abc* edge of f_1 joins the *ghi* edge of f_2:

f_2 facet symbol	numerical label	intrinsic label
a	12	$[f_2.f_6.f_7]$
b	13	$[f_2.f_7]$
c	14	$[f_2.f_7.f_8]$
d	15	$[f_2.f_8]$
e	16	$[f_2.f_8.f_3]$
f	17	$[f_2.f_3]$
g	18	$[f_2.f_3.f_1]$
h	19	$[f_2.f_1]$
i	20	$[f_1.f_5.f_6]$
j	21	$[f_2.f_6]$
k	22	$[f_2]$

In general, we can label the remaining facets in such a way that the

basic moves are, as permutations, given by:

$$f_1 = (1\ 3\ 5\ 7\ 9)(2\ 4\ 6\ 8\ 10)(20\ 31\ 42\ 53\ 64)\times$$
$$\times(19\ 30\ 41\ 52\ 63)(18\ 29\ 40\ 51\ 62)$$
$$f_2 = (12\ 14\ 16\ 18\ 20)(13\ 15\ 17\ 19\ 21)(1\ 60\ 73\ 84\ 31)\times$$
$$\times(3\ 62\ 75\ 86\ 23)(2\ 61\ 74\ 85\ 32)$$
$$f_3 = (23\ 25\ 27\ 29\ 31)(24\ 26\ 28\ 30\ 32)(82\ 95\ 42\ 3\ 16)\times$$
$$\times(83\ 96\ 43\ 4\ 17)(84\ 97\ 34\ 5\ 18)$$
$$f_4 = (34\ 36\ 38\ 40\ 42)(35\ 37\ 39\ 41\ 43)(27\ 93\ 106\ 53\ 5)\times$$
$$\times(28\ 94\ 107\ 54\ 6)(29\ 95\ 108\ 45\ 7)$$
$$f_5 = (45\ 47\ 49\ 51\ 53)(46\ 48\ 50\ 52\ 54)(38\ 104\ 117\ 64\ 7)\times$$
$$\times(39\ 105\ 118\ 65\ 8)(40\ 106\ 119\ 56\ 9)$$
$$f_6 = (56\ 58\ 60\ 62\ 64)(57\ 59\ 61\ 63\ 65)(49\ 115\ 75\ 20\ 9)\times$$
$$\times(50\ 116\ 76\ 21\ 10)(51\ 117\ 67\ 12\ 1)$$
$$f_7 = (67\ 69\ 71\ 73\ 75)(68\ 70\ 72\ 74\ 76)(58\ 113\ 126\ 86\ 12)\times$$
$$\times(59\ 114\ 127\ 7\ 13)(60\ 115\ 128\ 78\ 14)$$

$$f_8 = (78\ 80\ 82\ 84\ 86)(79\ 81\ 83\ 85\ 87)(71\ 124\ 97\ 23\ 14)\times$$
$$\times(72\ 125\ 98\ 24\ 15)(73\ 126\ 89\ 25\ 16)$$
$$f_9 = (89\ 91\ 93\ 95\ 97)(90\ 92\ 94\ 96\ 98)(80\ 122\ 108\ 34\ 25)\times$$
$$\times(81\ 123\ 109\ 35\ 26)(82\ 124\ 100\ 36\ 27)$$
$$f_{10} = (100\ 102\ 104\ 106\ 108)(101\ 103\ 105\ 107\ 109)\times$$
$$\times(91\ 130\ 119\ 45\ 36)(92\ 131\ 120\ 46\ 37)(93\ 122\ 111\ 47\ 38)$$
$$f_{11} = (111\ 113\ 115\ 117\ 119)(112\ 114\ 116\ 118\ 120)\times$$
$$\times(102\ 128\ 67\ 56\ 47)(103\ 129\ 68\ 57\ 48)\times$$
$$\times(104\ 130\ 69\ 58\ 49)$$
$$f_{12} = (122\ 124\ 126\ 128\ 130)(123\ 125\ 127\ 129\ 131)\times$$
$$\times(100\ 89\ 78\ 69\ 111)(101\ 90\ 79\ 70\ 112)(102\ 91\ 80\ 71\ 113)$$

4.9 Other permutation puzzles

I have left out several puzzles: "topspin" and "turnstile" (planar puzzles), "mozaika" (an equator-like puzzle, but the hemispheres may be rotated independently), "alexander's star" (a stellated icosahedron), "the "impossiball" (a spherically shaped icosahedron - see [H]), "mickey's challenge" (a spherically shaped irregular polyhedron - essentially the same as the skewb but with some added orientations of faces).

The puzzle "Christoph's jewel", essentially a "Rubik octahedron", may be solved using "super-Rubik's cube moves" (see [H]). (Indeed, one may take

a Rubik's cube, strip off all the stickers (using soap and water), and replace them with new stickers modeling a Rubik octahedron. This is because the octahedron is the dual solid of the cube, as described in chapter 7 below "Symmetry groups of the Platonic solids".)

The "orbix" puzzle (a battery run puzzle which has 12 buttons which light up) is a permutation puzzle if you think of a move (which switches certain of the buttons on/off) as permuting the elements of the set of all subsets of the 12 buttons (the subset of buttons which are lit) amongst themselves.

There is some mention of such puzzles in, for example, [Si], [H], [B], [GT] and [Jwww].

Chapter 5

Groups, I

Q: "What's commutative and purple?"
A: "An abelian grape".
— *Ancient Math Joke*

"In 1910 the mathematician Oswald Veblen and the physicist James Jeans were discussing the reform of the mathematical curriculum at Princeton University. 'We may as well cut out group theory,' said Jeans. 'That is a subject which will never be of any use to physics.' It is not recorded whether Veblen disputed Jeans' point, or whether he argued for the retention of group theory on purely mathematical grounds. All we know is that group theory continued to be taught. And Veblen's disregard for Jeans' advice continued to be of some importance to the history of science at Princeton. By the irony of fate group theory later grew into one of the central themes of physics, and it still dominates the thinking of all of us who are struggling to understand the fundamental particles of nature."
Freeman J. Dyson
SCIENTIFIC AMERICAN, Sep, 1964

When we studied permuation puzzles in Chapter 4, recall that one of the criteria was that each move was "invertible". This is, in fact, one of the conditions for the set of all legal moves of a permutation puzzle to form a group. A group is a set G with a binary operation (namely a function $* : G \times G \to$) satisfying certain properties to be given later, one of which is

that each element has an inverse element associated to it. One should be a little careful, since not every permutation puzzle gives rise to a group in this way. For example, the set of moves of the 15 puzzle do not form a group in this way though the set of moves of the Rubik's cube group do.

Just as for sets, we must decide on how to describe a group. If G is finite then one way is to list all the elements in G and list (or tabulate) all the values of the function $*$. Another method is to describe G in terms of some properties and then define a binary operation $*$ on G. A third method is to give a "presentation" of G. Each of these has its advantages and disadvantages. We shall eventually introduce all three of these approaches.

First, we start with an example.

5.1 The symmetric group

Before defining anything, we shall provide a little motivation for some general notions which will arise later.

Let X be any finite set and let S_X denote the set of all permutations of X onto itself:

$$S_X = \{f : X \to X \mid f \text{ is a bijection}\}.$$

This set has the following properties:

1. if f, g belong to S_X then fg (the composition of these permutations) also belongs to S_X, ("closed under compositions"),
2. if f, g, h all belong to S_X then $(fg)h = f(gh)$, ("associativity"),
3. the identity permutation $I : X \to X$ belongs to S_X ("existence of the identity"),
4. if f belongs to S_X then the inverse permutation f^{-1} also belongs to S_X ("existence of the inverse").

The set S_X is called the symmetric group of X. We shall usually take for the set X a set of the form $\{1, 2, ..., n\}$, in which case we shall denote the symmetric group by S_n. This group is also called the symmetric group on n letters.

Example 62. : Suppose $X = \{1, 2, 3\}$. We can describe S_X as

$$S_X = \{I, s_1 = (1\ 2), s_2 = (2\ 3), s_3 = (1\ 3\ 2), s_4 = (1\ 2\ 3), s_5 = (1\ 3)\}.$$

We can compute all possible products of two elements of the group and tabulate them in a multiplication table is

	I	s_1	s_2	s_3	s_4	s_5
I	I	s_1	s_2	s_3	s_4	s_5
s_1	s_1	I	s_3	s_2	s_5	s_4
s_2	s_2	s_4	I	s_5	s_1	s_3
s_3	s_3	s_5	s_1	s_4	I	s_2
s_4	s_4	s_2	s_5	I	s_3	s_1
s_5	s_5	s_3	s_4	s_1	s_2	I

Exercise 5.1.1. Verify the four properties of S_X mentioned above. (Note that the verification of associativity follows from the associative property of the composition of functions - see the Exercise 3.0.4).

5.2 General definitions

We take the above four properties of the symmetric group as the four defining properties of a group:

Definition 63. Let G be a set and suppose that there is a mapping

$$\begin{aligned} * : G \times G &\times G \\ (g_1, g_2) &\longmapsto g_1 * g_2 \end{aligned}$$

(called the group's operation) satisfying

(G1) if g_1, g_2 belong to G thn $g_1 * g_2$ belongs to G ("G is closed under $*$"),

(G2) if g_1, g_2, g_3 belong to G then $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ ("associativity"),

(G3) there is an element $1 \in G$ such that $1 * g = g * 1 = g$ for all $g \in G$ ("existence of an identity"),

(G4) if g belongs to G then there is an element $g^{-1} \in G$, called the inverse of g such that $g * g^{-1} = g^{-1} * g = 1$ ("existence of inverse").

Then G (along with the operation $*$) is a group.

Example 64. Actually, this is a "non-example". Let S be the set of all legal moves (one can eventually make from a legally obtained position) of the 15 puzzle (as described in Chapter 4). In a given position, for example the solved position, there aren't that many possibilities: there are only 2 moves in the solved position and there are never any more that 4 moves possible from any position.

From the solved position one can move $(15, 16)$ and $(12, 16)$ (where 16 denotes the blank square) but not for example $(1, 16)$. Since $(15, 16), (1, 16) \in S$ and since $(1, 16)(15, 16)$ is not a legal move, it follows that composition of legal moves is not always legal. This shows that composition is not a binary operation, so property number (G1) fails to hold.

In the above definition, we have not assumed that there was exactly one identity element 1 of G because, in fact, one can show that if there is one then it is unique. (To do this you need to use the cancellation law: if $a * c = b * c$, where $a, b, c \in G$, then $a = b$.) Likewise, if G is a group and $g \in G$ then the inverse element of g is unique. There are other properties of a group which can be derived from (G1)-(G4). We shall prove them as needed.

The multiplication table of a finite group G is a tabulation of the values of the binary operation $*$. Let $G = \{g_1, ..., g_n\}$. The multiplication table of G is:

$*$	g_1	g_2	...	g_j	...	g_n
g_1						
g_2						
$\vdots$						
g_i				$g_i * g_j$		
$\vdots$						
g_n						

Some properties:

Lemma 65. *(a) Each element $g_k \in G$ occurs exactly once in each row of the table.*

(b) Each element $g_k \in G$ occurs exactly once in each column of the table.

(c) If the $(i, j)^{th}$ entry of the table is equal to the $(j, i)^{th}$ entry then $g_i * g_j = g_j * g_i$.

(d) If the table is symmetric about the diagonal then $g * h = h * g$ for all $g, h \in G$. (In this case, we call G abelian.)

Example 66. Let C_{12} be the group whose elements are $\{0, 1, ..., 11\}$ and for which the group operation is simply "addition mod 12", just as one adds time on a clock (except that we call "12 o'clock" "0 o'clock"). Thus $5 + 8 = 1$, $1 + 11 = 0$, and so on.

Question: What is the inverse element of 5? The inverse of 1?

This group is called the cyclic group of order 12.

Exercise 5.2.1. Compute the multiplication table for C_{12}.

Definition 67. Let $n > 1$ be an integer and let C_n be the group whose elements are $\{0, 1, ..., n-1\}$ (more precisely, $\{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, where $\overline{i}$ is the residue class mod n of i) and for which the group operation is simply "addition mod n". This group is called the cyclic group of order n.

For further details on cyclic groups, see for example [G] or [R].

Definition 68. Let g and h be two elements of a group G. We say that g commutes with h (or that g, h commute) if $g * h = h * g$. We call a group commutative (or "abelian") if every pair of elements g, h belonging to G commute. If G is a group which is not necessarily commutative then we call G noncommutative (or "nonabelian").

Example 69. The integers, with ordinary addition as the group operation, is an abelian group.

Exercise 5.2.2. Show that any group having exactly 2 elements is abelian.

Now the reader should understand the punchline to the joke quoted at the beginning!

Convention: When dealing with groups in general we often drop the $*$ and denote multiplication simply by juxtaposition (that is, sometimes we write gh in place of $g * h$), with one exception. If the group G is abelian then one often replaces $*$ by $+$ and then $+$ is *not* dropped.

Now that we know the definition of a group, the question arises: how might they be described? The simplest answer is that we describe a group much as we might describe a set: we could list all its elements and give the multiplication table or we could describe all its elements and their multiplication in terms of some property from which we can verify the four properties of group. Though the first way has the distinct advantage of being explicit, it is this second alternative which is the most common since it is usually more concise.

Our objective is to introduce terminology and techniques which enable us to analyse mathematically permutation puzzles. The type of groups which arise in this context are defined next.

Definition 70. Let X be a finite set. Let $g_1, g_2, ..., g_n$ be a finite set of elements of permutations of X (so that they all belong to S_X). Let G be the set of all possible products of the form

$$g = x_1 * x_2 ... * x_m, \qquad m > 0,$$

where each of the $x_1, ..., x_m$ is taken from the set $\{g_1, ..., g_n\}$. The set G, together with the group operation given by composition of permutations, is called a permutation group with generators $g_1, ..., g_n$. We sometimes write

$$G =< g_1, ..., g_n >\subset S_X.$$

It is not too hard to justify our terminology:

Lemma 71. *A permutation group is a group.*

proof: Let G be a permutation group as in the above definition. We shall only prove that each $g \in G$ has an inverse, leaving the remainder of the properties for the reader to verify.

The set $\{g^n \mid n \geq 1\} \subset S_X$ is finite. There are $n_1 > 0$, $n_2 > n_1$ such that $g^{n_1} = g^{n_2}$. Then $g^{-1} = g^{n_2 - n_1 - 1}$ since $g \cdot g^{n_2 - n_1 - 1} = 1$. □

Remark 3. The above definition can be generalized: Replace S_X by any group S which includes all the generators $g_1, ..., g_n$. The resulting set G is called the group generated by the elements $g_1, ..., g_n$.

Algorithm:
Input: The generators $g_1, ..., g_n$ (as permutations in S_X),
Output: The elements of G,
$S = \{g_1, ..., g_n, g_1^{-1}, ..., g_n^{-1}\}$,
$L = S \cup \{1\}$,

```
for g in S do
  for h in L do
   if g*h not in L then L = L union {g*h} endif
  endfor
endfor
```

Note that the size of the list L in the for loop changes after each iteration of the loop. The meaning of this is that the if-then command is to be executed exactly once for each element of the list.

Exercise 5.2.3. Verify that permutation group G satisfies the four properties of a group (G1)-(G4).

Definition 72. If G is a group then the order of G, denoted $|G|$, is the number of elements of G. If g is an element of the group G then the order of g, denoted $ord(g)$, is the smallest positive integer m such that $g^m = 1$, if it exists. If such an integer m does not exist then we say that g has "infinite order".

Example 73. For example, there is an even permutation of order 42 in S_{12}, for example $(1,2)(3,4,5)(6,7,8,9,10,11,12)$, and an odd permutation of order 15 in S_8, for example $(1,2,3)(4,5,6,7,8)$.

Singmaster [Si] states that the maximal order in the Rubik's cube group is 1260.

We shall be able to make use of the following fact frequently.

Theorem 74. *(a) (Cauchy) Let p be a prime dividing $|G|$. There is a $g \in G$ of order p.*

(b) (Lagrange) Let n be an integer not dividing $|G|$. There does not exist a $g \in G$ of order n.

This will be proven a little later.

As an application of this: we shall see later that the Rubik's cube group G has the property that $|G| = 2^{27}3^{14}5^37^211$. It follows from this and Lagrange's theorem that there is no move of the Rubik's cube of order 13 but there is one of order 11.

Exercise 5.2.4. Let $X = \{1,2,3\}$. We use the notation of the example above.

(a) Let G be the permutation group with generator $s_1, G =< s_1 >$. Verify that there are only two elements in G.

(b) What is the order of s_5?

(c) Let G be the permutation group with generator $s_3, G =< s_3 >$. Verify that there are only three elements in G.

(d) Find the order of s_3.

(e) Show that $S_X =< s_1, s_2 >$.

Definition 75. If G is a permutation group G with only one generator then we say that G is cyclic.

Lemma 76. *If $G =< g >$ is cyclic with generator g then $|G| = ord(g)$.*

proof: Let $m = ord(g)$, so $g^m = 1$. We can list all the elements of G as follows:

$$1, g, g^2, ..., g^{m-1}.$$

There are m elements in this list. □

5.2.1 The Gordon game

Let G be a finite group, written

$$G = \{g_0 = 1, g_1, ..., g_n\}.$$

You and your opponent share a set of move tokens, denoted

$$M = \{g_1, ..., g_n\},$$

and place tokens, denoted

$$P = \{g_1, ..., g_n\}.$$

Rules to play:

- Players alternate turns. Each turn consists of removing one move token and one place token according to the conditions listed below. The first person who cannot make a legal play loses.

  Let $m_0 = p_0 = 1$ and let $i = 1$.

- First player picks any move token $m_1 \in M$ and the place token $p_1 = m_1 \in P$. These tokens m_1 and p_1 are then removed from M and P, resp..

- The next player picks any move token m_{i+1} such that $p_{i+1} = m_{i+1}p_i \in P$. These tokens m_{i+1} and p_{i+1} are then removed from M and P, resp..

- Increment i and go to the previous step.

Example 77. Let

$$G = \mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

The moves of a game are determined by recording the move tokens. One possible game is

$$\begin{array}{ccccccccc} \bullet & 4 & 1 & & & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

where the $\bullet$ over the identity element 0 of the group indicates that it isn't moved and the numbers above a group element indicates when it was moved:

$$\begin{gathered} 1^{st}\text{: } m_1 = 2,\ p_1 = 2;\ 2^{nd}\text{: } m_2 = 4,\ p_2 = 6; \\ 1^{st}\text{: } m_3 = 6,\ p_3 = 5;\ 2^{nd}\text{: } m_4 = 3,\ p_4 = 1; \\ 2^{nd} \text{ player wins} \end{gathered}$$

Exercise 5.2.5. Play a game!

Remark 4. If $G = \mathbb{Z}/p\mathbb{Z}$ (the cyclic group with p elements) there is a conjecture that the 2^{nd} player has a winning strategy when $p > 5$ (see Isbell's note [I]). In general, strategies are not not only not known, they haven't even been conjectured.

Remark 5. If you and your opponent both try to drag the game on as long as possible, can you exhaust the set of move tokens and the set of place tokens? The answer is known for abelian groups, dihedral groups and groups of order < 32. The general answer is unknown.

5.3 Subgroups

Definition 78. Let G be a group. A subgroup of G is a subset H of G such that H, together with the operation $*$ inherited as a subset of G, satisfies the group operations (G1)-(G4) (with G replaced by H everywhere).

Notation: If G is a group then we will denote the statement "H is a subgroup of G" by

$$H < G.$$

Problem: What are the subgroups of the Rubik's cube group? It turns out that there are too many to list but later, when we have a more useful way of describing a group (using generators and relations - see §9.3), we will explicitly determine some of the subgroups of "small" order.

Theorem 79. *(Lagrange) Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$.*

proof: For $x, y \in G$, define $x \sim y$ if $xH = yH$, where

$$xH = \{x * h \mid h \in H\}.$$

This is an equivalence relation (Exercise: Check reflexive, symmetry, and transitivity). Moreover, the equivalence class of x consists of all elements in G of the form $x * h$, for some $h \in H$, i.e., $[x] = xH$. Let $g_1, ..., g_m \in G$ denote a complete set of representatives for the equivalence classes of G. Because of the cancellation law for groups, $|xH| = |H|$ for each $x \in G$. Furthermore, we know that the equivalence classes partition G, so

$$G = \cup_{i=1}^{m} [g_i] = \cup_{i=1}^{m} g_i H.$$

Comparing cardinalities of both sides, we obtain $|G| = |g_1 H| + ... + |g_m H| = m|H|$. This proves the theorem. □

Definition 80. If H and G are finite groups and $H < G$ then the integer $|G|/|H|$ is called the index of H in G, denoted $[G : H] = |G|/|H|$.

Exercise 5.3.1. Show, as a corollary to the previous Theorem 79, that Theorem 74 is true.

Example 81. A permutation group G generated by elements $g_1, ..., g_n$ belonging to S_X is a subgroup of S_X, i.e., $G < S_X$.

Example 82. Let

$$A_X = \{g \in S_X \mid g \text{ is even}\}.$$

This is a subgroup of S_n called the alternating subgroup of degree n .

Definition 83. The center of a group G is the subgroup $Z(G)$ of all elements which commute with every element of G:

$$Z(G) = \{z \in G \mid z * g = g * z, \text{ for all } g \in G\}.$$

Of course, the identity element always belongs to G. If the identity element is the only element of $Z(G)$ then we say G has trivial center. On the other hand, G is commutative if and only if $G = Z(G)$.

Exercise 5.3.2. Let $G = S_3$. Determine $Z(G)$.

5.4 Examples of groups

Example 84. The collection of all moves of the 15 puzzle may be viewed as a subgroup of S_{16}.

Example 85. The collection of all moves of the Rubik's cube may be viewed as a subgroup G of S_{48}. The center of G consists of exactly two elements, the identity and the "superflip" move which has the effect of flipping over every edge, leaving all the corners alone and leaving all the subcubes in their original position. One move for the superflip is

$$\begin{aligned}\text{superflip} = R*L*F*B*U*D*R*L*F*B*U*F^2*M_R* \\ *F^2*U^{-1}*M_R^2*B^2*M_R^{-1}*B^2*U*M_R^2*D,\end{aligned}$$

where M_R is middle right slice rotation by 90 degrees (viewed from the right face). The proof of this fact uses the determination of the group structure of G given later (see also [B]).

5.4.1 The dihedral group

Pick an integer $n > 2$ and let R be a regular n-gon centered about the origin in the plane. If $n = 3$ then R is an equilateral triangle, if $n = 4$ then R is a square, if $n = 5$ then R is a pentagon, and so on. Let G denote the set of all linear transformations of the plane [1] to itself which preserve the figure R. The binary operation $\circ : G \times G \to G$ given by composition of functions gives G the structure of a group. This group is called the group of symmetries of R.

Label the vertices of the n-gon as 1, 2, ..., n. The group G permutes these vertices amongst themselves, hence each $g \in G$ may be regarded as a permutation of the set of vertices $V = \{1, 2, ..., n\}$. In this way, we may regard G as a permutation group since it is the subgroup of S_n generated by the elements of G.

The fact that this group has $2n$ elements follows from a simple counting argument: Let $r \in G$ denote the element which rotates R by $2\pi/n$ radians counterclockwise about the center. Let L be a line of symmetry of R which bisects the figure into two halves. Let s denote the element of G which is reflection about L. There are n rotations by a multiple of $2\pi/n$ radians

[1] If we regard R as a figure in 3-space centered above the origin and let G denote the set of all linear transformations *of* 3-*space* then we obtain a slightly larger group in some cases [NST].

about the center in G: $1, r, r^2, ..., r^{n-1}$. There are n elements of G which are composed of a reflection about L and a rotations by a multiple of $2\pi/n$ radians about the center: $s, s \circ r, s \circ r^2, ..., s \circ r^{n-1}$. These comprise all the elements of G.

One remarkable property of this symmetry group, which we shall use in the example in the next section, is that it is generated by any two distinct reflections in the group:

Lemma 86. *Pick two distinct lines L, L' of symmetries of R, each of which bisects R in half, and let s, s' (resp.) denote the corresponding reflections, regarded as elements in S_n. Then $G =< s, s' >$.*

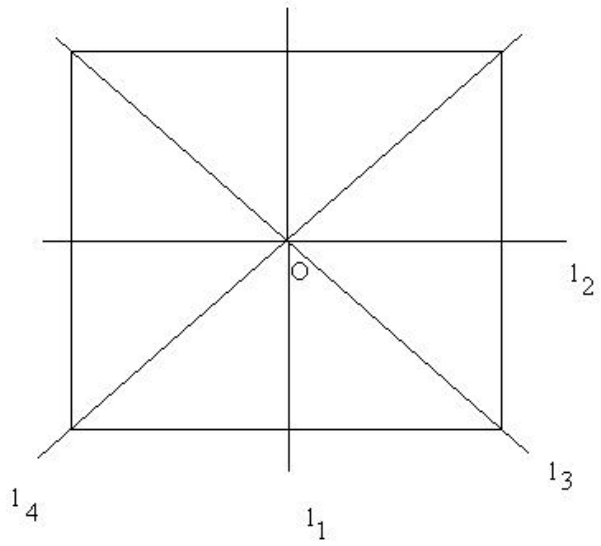
The interested reader is referred to [NST], [R], or [Ar], chapter 5, §3, for a proof.

The symmetry group of R is known as the dihedral group of order $2n$, denoted D_{2n}. We shall state the precise relation in a later chapter (chapter 8) after we have introduced more terminology.

Example 87. Let G be the symmetry group of the square: i.e., the group of symmetries of the square generated by the rigid motions

$$\begin{aligned} g_0 = 90 \text{ degrees clockwise rotation about O}, \\ g_1 = \text{reflection about } \ell_1, \\ g_2 = \text{reflection about } \ell_2, \\ g_3 = \text{reflection about } \ell_3, \\ g_4 = \text{reflection about } \ell_4, \end{aligned}$$

where ℓ_1, ℓ_2, ℓ_3 denote the lines of symmetry in the picture below:



The elements of G are

$$1, g_0, g_0^2, g_0^3, g_1, g_2, g_3, g_4.$$

Let X be the set of vertices of the square. Then G acts on X.

5.4.2 Example: The two squares group

This material is based on an idea mentioned in [FS].

Let $H =< R^2, U^2 >$ denote the group generated by the two square moves, R^2 and U^2 or the Rubik's cube. (The reader with a cube in hand may want to try the Singmaster magic grip : the thumb and forefinger of the right hand are placed on the front and back face of the fr, br edge, the thumb and forefinger of the left hand are placed on the front and back face of the uf, ub edge; all moves in this group can be made without taking your fingers off the cube.) This group contains the useful 2-pair edge swap move $(R^2 * U^2)^3$.

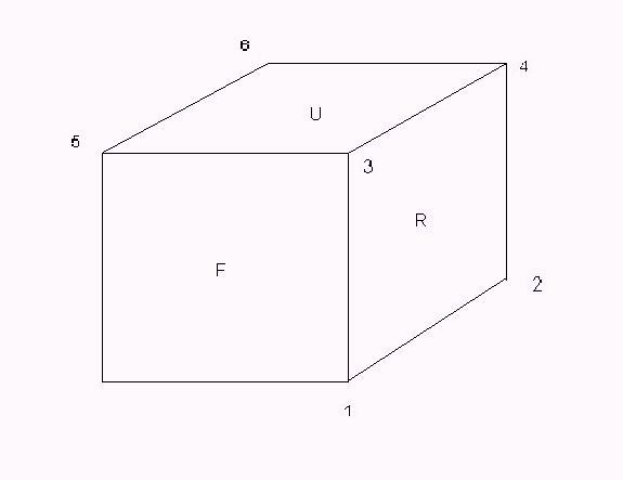
We can find all the elements in this group fairly easily:

$$H = \{1, R^2, R^2 * U^2, R^2 * U^2 * R^2, (R^2 * U^2)^2, (R^2 * U^2)^2 * R^2, (R^2 * U^2)^3,$$
$$(R^2 * U^2)^3 * R^2, (R^2 * U^2)^4, (R^2 * U^2)^4 * R^2, (R^2 * U^2)^5, (R^2 * U^2)^5 * R^2\},$$

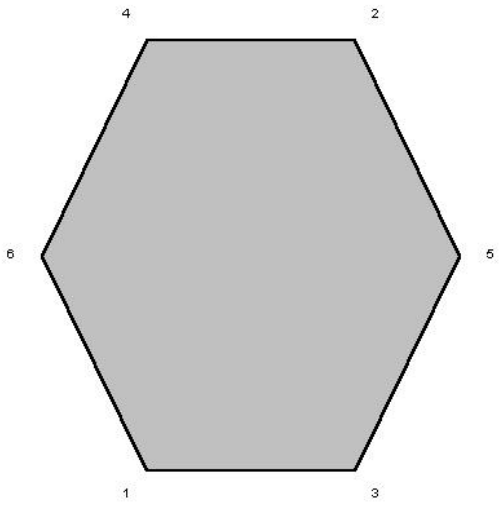
Therefore, $|H| = 12$. Note that $1 = (R^2 * U^2)^6$, $U^2 = (R^2 * U^2)^5 * R^2$, and $U^2 * R^2 = (R^2 * U^2)^5$. (By the way, this listing without repetition of H by

successive multiplication by R^2 then U^2 may be reformulated graphically by saying the "the Cayley graph of H with generators R^2, U^2 has a Hamiltonian circuit". This interpretation will be discussed in the next chapter.)

To discover more about this group, we label the vertices of the cube as follows:



The move R^2 acts on the set of vertices by the permutation (1 4)(2 3) and the move U^2 acts on the set of vertices by the permutation (4 5)(3 6). We label the vertices of a hexagon as follows:



The permutation (1 4)(2 3) is simply the reflection about the line of symmetry containing both 5 and 6. The permutation (4 5)(3 6) is simply the reflection about the line of symmetry containing both 1 and 2. By a fact stated in section 5.4.1, these two reflections generate the symmetry group of the hexagon.

5.5 Commutators

Definition 88. If g, h are two elements of a group G then we call the element

$$[g, h] = g * h * g^{-1} * h^{-1}$$

then commutator of g, h.

Not that $[g, h] = 1$ if and only if g, h commute. Thus the commutator may be regarded as a rough measurement of the lack of commutativity.

Exercise 5.5.1. Let $G = S_3$, the symmetric group on 3 letters. Compute the commutators

$$[s_1, s_2], \quad [s_2, s_1].$$

Exercise 5.5.2. Let R, U be as in the notation for the Rubik's cube moves introduced in the previous chapter. Determine the order of the move $[R, U]$. (Ans: 6)

Definition 89. (Singmaster [Si]) Let G be the permutation group generated by the permutations R, L, U, D, F, B regarded as permutations in S_{54}. The Y commutator is the element

$$[F, R^{-1}] = F * R^{-1} * F^{-1} * R.$$

The Z commutator is the element

$$[F, R] = F * R * F^{-1} * R^{-1}.$$

Exercise 5.5.3. (a) Find the orders of the Y commutator and the Z commutator.

(b) Find the order of $[R, [F, U]]$.

Example 90. If x, y are basic moves of the Rubik's cube associated to faces which share an edge then

(a) $[x, y]^2$ permutes exactly 3 edges and does not permute any corners,

(b) $[x, y]^3$ permutes exactly 2 pairs of corners and does not permute any edges.

Definition 91. Let G be any group. The group G' generated by all the commutators

$$\{[g, h] \mid g, h \text{ belong to } G\}$$

This is called the commutator subgroup of G.

This group may be regarded as a rough measurement of the lack of commutativity of the group G.

Remark 6. We will see later that the group generated by the basic moves of the Rubik's cube - R, L, U, D, F, B - has a relatively large commutator subgroup. In other words, roughly speaking "most" moves of the Rubik's cube can be generated by commutators such as the Y commutator or the Z commutator.

Definition 92. If we repeatedly take commutator subgroups we get a series of groups G, G', $G'' = (G')'$, and so on. The derived series of a group G is the sequence of subgroups

$$... < (G')' < G' < G.$$

A group G is called solvable if one of the groups in the derived series is the trivial group consisting only of the identity.

Exercise 5.5.4. Let G be an abelian group. Show that G is solvable.

5.6 Conjugation

Definition 93. : If g, h are two elements of a group G then we call the element

$$g^h = h^{-1} * g * h$$

the conjugation of g by h.

Note that $g^h = 1$ if and only if g, h commute. Thus the conjugates may be regarded as a rough measurement of the lack of commutativity.

Exercise 5.6.1. Show $g * [g^{-1}, h^{-1}] = g^h$.

Exercise 5.6.2. Let $G = S_3$, the symmetric group on 3 letters, in the notation of the example above. Compute the conjugations

$$s_1^{s_2}, \qquad s_2^{s_1}.$$

Exercise 5.6.3. Let R, U be as in the notation for the Rubik's cube moves introduced in the previous chapter. Determine the order of the move R^U. (Ans: 4)

Definition 94. : We say two elements g_1, g_2 of G are conjugate if there is an element $h \in G$ such that $g_2 = g_1^h$.

It turns out that it is easy to see when two permutations $g, h \in S_n$ are conjugate: they are conjugate if and only if the cycles in their respective disjoint cycle decompositions have the same length when assanged from shortest to longest. For example, the elements

$$g = (6,9)(1,3,4)(2,5,7,8), \qquad h = (1,2)(3,4,5)(6,7,8,9)$$

are conjugate. We shall leave the details and the proof for later - see §8.3.1

Exercise 5.6.4. Show that the notion of conjugate defines an equivalence relation. That is, show that

(a) any element $g \in G$ is conjugate to itself ("reflexive"),

(b) if g is conjugate to h (g, h belonging to G) then h is conjugate to g ("symmetry"),

(c) if g_1 is conjugate to g_2 and g_2 is conjugate to g_3 then g_1 is conjugate to g_3 ("transitivity").

Notation: The set of equivalence classes of G under the equivalence relation given by conjugation, will be denoted G_*.

The polynomial

$$p_G(t) = \sum_{g \in G_*} t^{ord(g)},$$

is called the generating polynomial of the order function on G. Note two elements which are conjugate must have the same order since $(h^{-1}gh)^n = (h^{-1}gh)(h^{-1}gh)...(h^{-1}gh) = h^{-1}g^nh$, for $n = 1, 2, ...$ and $g, h \in G$.

In [Si], §5.10D, D. Singmaster asks for the possible orders of the elements of the Rubik's cube group and how many elements of each order there are.

(A method for determining this will be described later in this text.) This question of Singmaster motivates the following:

Problem: Determine $p_G(t)$ for the Rubik's cube group.

Example 95. For S_8, the generating polynomial is

$$t + 4t^2 + 2t^3 + 4t^4 + t^5 + 5t^6 + t^7 + t^8 + t^{10} + t^{12} + t^{15}$$

and for S_{12} it is

$$t + 6t^2 + 4t^3 + 9t^4 + 2t^5 + 16t^6 + t^7 + 4t^8 + 2t^9 + 6t^{10} + t^{11} + 9t^{12} + 2t^{14} + 2t^{15} + t^{18} + 2t^{20} + t^{21} + t^{24} + t^{28} + 3t^{30} + t^{35} + t^{42} + t^{60}.$$

(Both of these calculations were performed by MAPLE.) For example, it follows that there is an even permutation of order 42 in S_{12} and an odd permutation of order 15 in S_8.

Singmaster [Si] states that the maximal order in the Rubik's cube group is 1260.

Definition 96. : Fix an element g in a group G. The set

$$Cl(g) = \{h^{-1} * g * h \mid h \in G\}$$

is called the conjugacy class of g in G. It is the equivalence class of the element g under the relation given by conjugation.

If H is a subgroup of G and if g is a fixed element of G then the set

$$H^g = \{g^{-1} * h * g \mid h \in H\}$$

is a subgroup of G. Such a subgroup of G is called a subgroup conjugate to H.

Exercise 5.6.5. Let S be the set of all subgroups of G. We define a relation R on S by

$$R = \{(H_1, H_2) \in S \times S \mid H_1 \text{ is conjugate to } H_2\}.$$

Show that R is an equivalence relation.

Exercise 5.6.6. Let $G = S_n$ and let $H =< g >$ be a cyclic subgroup generated by a permutation g of the set $\{1, 2, ..., n\}$. With respect to the equivalence relation in the previous exercise, show that a subgroup K of G belongs to the equivalence class $[H]$ of H in G if any only if K is cyclic and is generated by an element k of G conjugate to $g \in G$.

5.7 Orbits and actions

Definition 97. Let X be a set and let G be a group. We call X a G-set and we say G acts on X provided the following conditions hold:

1. each g belonging to G gives rise to a function
$$\phi_g : X \to X,$$
2. the identity 1 of the group G defines the identity function on X,
3. if g, h belong to G then the composite
$$\phi_{gh} : X \to X$$
satisfies $\phi_{gh}(x) = \phi_h(\phi_g(x))$.

We call this action a left action since the left-most element (namely, g) in the product gh acts first.

Similarly, we define

Definition 98. Let X be a set and let G be a group. We say G acts on X on the right provided the following conditions hold:

1. each g belonging to G gives rise to a function
$$\phi_g : X \to X,$$
2. the identity 1 of the group G defines the identity function on X,
3. if g, h belong to G then the composite
$$\phi_{gh} : X \to X$$
satisfies $\phi_{gh}(x) = \phi_g(\phi_h(x))$.

We call this action a right action since the right-most element (namely, h) in the product gh acts first.

Remark 7. (1) We shall see another interpretation of these definitions in the later chapter entitled, "Groups, II".

(2) Given a left action ϕ_g, one can create a right action by defining $\phi'_g = \phi_{g^{-1}}$.

Following the standard convention, the Rubik's cube will act on the set of facets of the cube on the right.

Definition 99. Let G act on a set X. We call the action transitive if for each pair x, y belonging to X there is a $g \in G$ such that $y = \phi_g(x)$.

In other words, a group G acts transitively on a set X if *any* element x of X can be send to *any* other element y of X by some element of G.

Example 100. Let X be a finite set and let $G = S_X$ be the symmetric group of X. Then X is a G-set and G acts transitively on X.

Exercise 5.7.1. Show that the action in the previous example is transitive.

Example 101. Let G be the group of all 2×2 invertible matrices with real entries, $G = GL_2(\mathbb{R})$. This group acts on the set of column vectors on the left.

Exercise 5.7.2. Let G be the permutation group generated by the permutations R, L, U, D, F, B, regarded as elements of S_{48}. Let E denote the set of edges of the cube, which we identify with the set of edge subcubes. Let V denote the set of vertices of the cube, which we identify with the set of corner subcubes of the cube. Let X be the set of all movable subcubes of the Rubik's cube (which may identify as the union of E and V). Then G acts on X, E and G acts on V.

Question (a) Is the action of G on X transitive?

(a) Is the action of G on E transitive?

(b) Is the action of G on V transitive?

Exercise 5.7.3. Let G be a group and let $X = G$. Define left multiplication of G on X by:

$$\begin{aligned} \phi_g : X &\to X \\ x &\longmapsto \phi_g(x) = g * x. \end{aligned}$$

(a) Show that left multiplication defines a left action of G on X.

(b) Show that this action is transitive.

(c) Show that each $\phi_g : G \to G$ is a permutation of the set G, so $\phi_g \in S_G$.

Exercise 5.7.4. Let G be a group and let $X = G$. Define right multiplication of G on X by:

$$\begin{aligned} \phi_g : X &\to X \\ x &\longmapsto \phi_g(x) = x * g. \end{aligned}$$

(a) Show that right multiplication defines a right action of G on X.

(b) Show that this action is transitive.

(c) Show that each $\phi_g : G \to G$ is a permutation of the set G, so $\phi_g \in S_G$.

Exercise 5.7.5. Let G be a group and let $X = G$. Define conjugation on X by:

$$\begin{array}{c} \phi_g : X \to X \\ x \longmapsto \phi_g(x) = g^{-1} * x * g. \end{array}$$

Show that conjugation defines an action of G on X (X and G as above).

Exercise 5.7.6. Let G be a group and let X denote the set of all *subgroups* of G. Define conjugation on X by:

$$\begin{array}{c} \phi_g : X \to X \\ x \longmapsto \phi_g(x) = g^{-1} * x * g. \end{array}$$

Show that this defines an action of G on X.

Remark 8. In general, the actions in the last two exercises are not transitive.

Definition 102. Let G be a group acting on a set X. For each x belonging to X, the set

$$G * x = \{\phi_g(x) \mid g \in G\}$$

is called the orbit of $x \in X$ under G.

Algorithm

Input: A set S of generators of a permutation group G and an x belonging to X

Output: The orbit of x, $G * x$

```
orbit = {x}
for y in orbit do
  for g in S do
    if g*y not in orbit then orbit = orbit union {g*y} endif
  endfor
endfor
```

Note that the size of the list orbit in the for loop changes after each iteration of the loop. As mentioned before, the meaning of this is that the if-then command is to be executed exactly once for each element of the list.

Exercise 5.7.7. Let G be the Rubik's cube group and let x be the uf edge facet. Find the orbit of x under the action of G using the above algorithm. Show each step.

Exercise 5.7.8. Let G be the group of moves of the Rubik's cube and let X be the set of vertices of the cube. Let H be the subgroup of G generated by $U * R$. Find:

(1) the order of $U * R$, (Ans: 105)

(2) the orbit (in the Singmaster notation) of the ufr vertex in X under H.

Definition 103. Let G be a group acting on a set X with the action denoted by ϕ. For each x belonging to X, the subgroup

$$stab_G(x) = G_x = \{g \in G \mid \phi_g(x) = x\}$$

is called the stabilizer of x in G.

Exercise 5.7.9. Let G be a group acting on a set X, $\phi_g : X \to X$, for all $g \in G$. Show that, for all $x \in X$ and all $g \in G$, we have $stab_G(\phi_g(x)) = g * stab_G(x) * g^{-1}$.

Example 104. Let G be the group of symmetries of the square (see the example above), let X be the set of vertices of the square, and let x_0 be the vertex in the lower right hand corner. Then $stab_G(x_0) =< g_3 >$.

Exercise 5.7.10. Let G be any group and let $X = G$. Let G act on X by left multiplication:

$$\phi_g : X \to X$$
$$x \longmapsto \phi_g(x) = g * x.$$

Show that

$$stab_G(x) = 1,$$

for all x belonging to $X = G$.

Exercise 5.7.11. Let G be any group and let $X = G$. Let G act on X by conjugation:

$$\phi_g : X \to X$$
$$x \longmapsto \phi_g(x) = g * x * g^{-1}.$$

Show that

$$stab_G(x) = \{g \in G \mid g * x = x * g\},$$

for all x belonging to $X = G$. (The subgroup

$$C_G(x) = \{g \in G \mid g * x = x * g\}$$

is called the centralizer of x in G.)

Example 105. Let X be the set of consisting of the 48 facets of the Rubik's cube which are not center facets - i.e., the "movable" facets. Let V denote the subset of facets which belong to some corner subcube, E the subset of facets which belong to some edge subcube. Let G denote the Rubik's cube group. As noted above, G acts on X, V, E. The action of G on X induced an equivalence relation as follows: we say that a facet f_1 is "equivalent" to a facet f_2 if there is an element of G (i.e., a move of the Rubik's cube) which sends one facet to the other. By exercise 5.7.2, there are exactly two equivalence classes, or orbits, of G in X: V and E. In particular, the action of G on V is transitive and the action of G on E is transitive.

5.8 Cosets

Let G be a group and H a subgroup of G. For g belonging to G, the subset $g * H$ of G is called a left coset of H in G and the subset $H * g$ of G is called a right coset of H in G.

Exercise 5.8.1. If H is finite, show $|H| = |g * H| = |H * g|$.

Exercise 5.8.2. If X is a left coset of H in G and x is an element of G, show that $x * X$ is also a left coset of H in G.

Notation: The set of all left cosets is written G/H and the set of all right cosets of H in G is denoted $H\backslash G$.

These two sets don't in general inherit a group structure from G but they are useful none-the-less. (G/H is a group with the "obvious" multiplication $(g_1 * H) * (g_2 * H) = (g1g_2) * H$ if and only if H is a "normal" subgroup of G - we will define "normal" below.)

As an example of their usefulness, we have the following relationship between the orbits and the cosets of the stabilizers.

Lemma 106. *Let G be a finite group acting on a set X. Then*

$$|G * x| = |G/stab_G(x)|,$$

for all x belonging to X.

proof: The map

$$g * stab_G(x) \longmapsto g * x$$

defines a function $f : G/stab_G(x) \to G * x$. This function is a bijection since it is both and injection (Exercise: Check this) and a surjection (Exercise: Check this). □

Exercise 5.8.3. Let G be the group of symmetries of the square. Using the notation above, compute $G/ < g_3 >$ and $G * x_0$.

Theorem 107. *(Lagrange): If G is a finite group and H a subgroup then*

$$|G/H| = |G|/|H|.$$

Corollary 108. *If H, G are as above then the order of H divides the order of G.*

proof of Theorem: Let X be the set of left cosets of H in G and let G act on X by left multiplication. Apply the previous lemma with $x = H$. □

Exercise 5.8.4. Let $G = S_3$, the symmetric group on 3 letters, and let $H =< s_1 >$, in the notation of §5.1 above.

(a) Compute $|G/H|$ using Lagrange's Theorem.

(b) Explicitly write down all the cosets of H in G.

Definition 109. : Let H be a subgroup of G and let C be a left coset of H in G. We call an element g of G a coset representative of C if $C = g * H$. A complete set of coset representatives is a subset of G, $x_1, x_2, ..., x_m$, such that

$$G/H = \{x_1 * H, ..., x_m * H\},$$

without repetition (i.e., all the $x_i * H$ are disjoint).

Exercise 5.8.5. For $g_1, g_2 \in G$, define $g_1 \sim g_2$ if and only if g_1 and g_2 belong to the same left coset of H in G.

(a) Show that $\sim$ is an equivalence relation.

(b) Show that the left cosets of H in G partition G.

5.9 Dimino's Algorithm

We saw in an earlier chapter an algorithm for computing all the elements of a permuation group G. We shall discuss a more efficient algorithm for doing this in this section. For more details, see [Bu].

Notation: Let $S = \{g_1, g_2, ..., g_n\}$ be a set of generators for a permutation group G. Let

$$S_0 = \emptyset,$$
$$S_i = \{g_1, ..., g_i\},$$
$$G_0 = \{1\},$$
$$G_i =< S_i >= \text{the group generated by the elements in } S_i,$$

for $1 \leq i \leq n$.

Algorithm (inductive step):

Input: The generators S of G and a list L of all the elements of the permutation subgroup G_{i-1}.

Output: A list L of elements of G_i and a list C of coset representatives of G_i/G_{i-1}.

```
C = {1}
for g in C do
 for s in S_i do
  if s*g not in L then
      C = C union {s*g}
      L = L union s*g*G_{i-1}
  endif
 endfor
endfor
```

Algorithm (Dimino):

Input: The generators S of G

Output: A list of elements of G

```
 (Initial case S_1 = <g1>)
order = 1, element[1] = 1, g = g1
while g <> 1 do
  order = order + 1
  element[order] = g
```

```
  g = g*g1
endwhile



 (General case)
for i from 2 to n do
  <insert inductive step here>
endfor
```

Example 110. Let $G = S_3 =< s_1, s_2 >$. We use Dimono's algorithm to list all the elements of G. We have

$$G_0 = \{1\} < G_1 =< s_1 >< G_2 = G.$$

First, we list the elements of $G_1 =< s_1 >$. Since $s_1 = (1\ 2)$, it is order 2, so

$$G_1 = \{1, s_1\}.$$

This is our list L which we will apply the "inductive step" of Dimino's algorithm to (with $i = 2$). We start with $C = \{1\}$. Now we look at the left cosets of G_1 in $G_2 = G$. We have (with $g = 1, s = s_1$)

$$s_1 * G_1 = G_1,$$

so we don't increase the size of C or L. Next, we have (with $g = 1, s = s_2$)

$$s_2 * G_1 = \{s_2, s_2 * s_1\} \neq G_1,$$

so $L = \{1, s_1, s_2, s_2 * s_1\}, C = \{1, s_2\}$. Next, we have (with $g = s_2, s = s_1$)

$$s_1 * s_2 * G_1 = \{s_1 * s_2, s_1 * s_2 * s_1\} \neq G_1.$$

(We know $s_1 * s_2 * G_1 \neq G_1$ since neither of the two elements in $s_1 * s_2 * G_1$ is the identity.) Thus, we increase L, C:

$$L = \{1, s_1, s_2, s_2 * s_1, s_1 * s_2, s_1 * s_2 * s_1\},$$

and $C = \{1, s_2, s_1 * s_2\}$. We know we may stop here since we know $|S_3| = 6$ but the algorithm still has one more statement to execute. Next, we have (with $g = s_2, s = s_2$)

$$s_2 * s_2 * G_1 = G_1,$$

so we don't increase the size of C or L (as expected). This step terminates the algorithm and $S_3 = L$.

Exercise 5.9.1. Perform Dimino's algorithm on

$$S_4 =< s_1 = (1\ 2), s_2 = (2\ 3), s_3 = (3\ 4) > .$$

5.10 Permutations and campanology

This section is based on a capstone project of S. Robinson [Rob].

Standing outside of Westminster Abbey as the bells chime, the result you hear may actually be much more mathematical, than musical. While your ears think they detect melody,they are being deceived. The bells are not being rung in melody at all; in actuality, they are being rung in permutations ([Wh], p771). Since the seventeenth century, and possibly before, cathedral bells in England have been rung by such permutations or changes ([Wh], p771). The art and study of such bell ringing is referred to as campanology. While campanology had been around for at least a century before the formalization of what is now known as group theory, elements of group theory are implicit in campanology.

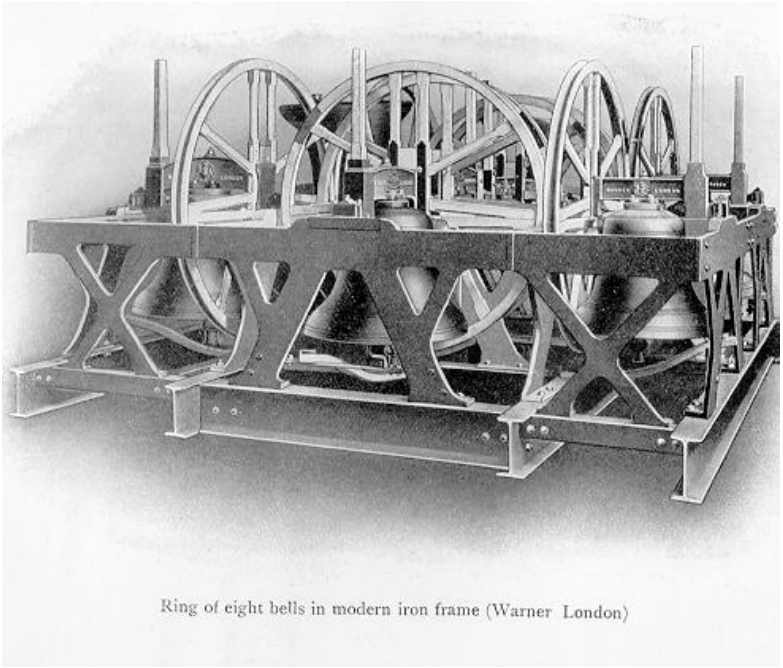
Fabian Stedman, referred to as "one of the 'fathers of bell ringing,'" is conjectured by Arthur White, to have been, perhaps, the first group theorist ([Wh], p771). Born in 1640 to Reverend Francis Stedman, Fabian Stedman's connections with campanology took root at the early age of 15 when he moved to London to work as an apprentice to a Master Printer. While in London Stedman joined a bell-ringing society known as the Scholars of Cheapside and served as the societies treasurer in 1662. In 1664, Stedman went on to join another bell-ringing society known then as the "Society of Colledg(sic) Youths," which has since been renamed the Ancient Society of College Youths and is still in existence today ([Wh], p771). Stedman remained with the society becoming Steward of College Youths in 1677 and eventually in 1682 Master of the Society. Stedman's major contributions to campanology are reflected in his efforts on Tintinnlogia and Campanalogia, the first two books published on the subject, in 1668 and 1677, respectively ([Wh], p771).

To leap right into a discussion of Stedman's work, campanology, or group theory even in their most general terms without some cursory definitions would be futile. Below is a glossary of a few essential terms:

- Transposition: a cycle (i,j) of length 2 which interchanges i and j
- Change: the swapping of one or more disjoint pairs of adjacent bells

- Plain change: involves swapping one pair of adjacent bells only
- Cross change: involves more than one swapping pair of bells
- Round: A unique ordering of the bells (i.e. $(1, 2, 3, ..., n)$)

The following picture was taken from [Wa], page 71.



Ring of eight bells in modern iron frame (Warner London)

In the beginning, change ringing concerned itself with a single row of bells whose order could be denoted by $(1, 2, 3, ..., n)$. Considering the case where $n = 6$ the concepts of plain and cross changes can be understood more clearly. If we use only plain changes we can generate permutations of the bells as follows:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5, \end{array}$$

It should be fairly obvious on inspection that the first plain change swaps 1 and 2, the second swaps 3 and 4, and the third swaps 5 and 6. Considering

the same set of six bells acted upon by a cross change, the same result is achieved in one change, as seen below:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5. \end{array}$$

More useful and interesting patterns can be generated by combining plain and cross changes. The plain lead on four bells is one of the most simplistic patterns and was devised sometime around 1621 by alternating consecutive cross and plain changes as seen below:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 1 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 3 & 1 & 4 & 2 \\ 1 & 3 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{array}$$

It is easy to see that the pattern which defines the plain lead on four bells is nothing more than a cross change followed by a plain change on the middle two bells until we reach the round, which is where we started. Generating the plain lead on four bells is analogous algebraically to generating the dihedral group on four elements, D_4. We begin by representing the cross change as $a = (1,2)(3,4)$ which swaps the first two and last two bells and representing the plain change as $b = (2,3)$ which swaps the middle pair. Algebraically, D_4 is generated by multiplication. We begin with the first element in the group, a. To generate the next element in the group we multiply this first element by b. To generate the third element we simply multiply this second term, ab, by a to get aba. Continuing on in this manner we multiply alternately by a then b to generate the dihedral group $D_4 = \{a, ab, aba, (ab)^2, a(ab)^2, (ab)^3, (ab)^3a, (ab)^4\}$. Since $(ab)^4$ yields the round, we say $(ab)^4 = 1$ and $D_4 = \{1, a, ab, aba, (ab)^2, a(ab)^2, (ab)^3, (ab)^3a\}$. While this simple example illustrates the implicit elements of group theory which seem to be at the heart of bell ringing, moving on to a more complex example illuminates perhaps more significant implications.

We turn our attention now to the composition which is commonly referred to as Plain Bob Minimus. Plain Bob Minimus begins at the round and ends at

the round $(1, 2, 3, 4)$ and contains all possible permutations of these four bells. Calling the earlier definitions to mind, it should be evident that generating the Plain Bon Minimus composition is equivalent algebraically to generating the symmetric group on 4 elements, S_4, which is shown:

1 2 3 4	1 3 4 2	1 4 2 3
2 1 4 3	3 1 2 4	4 1 3 2
2 4 1 3	3 2 1 4	4 3 1 2
4 2 3 1	2 3 4 1	3 4 2 1
4 3 2 1	2 4 3 1	3 2 4 1
3 4 1 2	4 2 1 3	2 3 1 4
3 1 4 2	4 1 2 3	2 1 3 4
1 3 2 4	1 4 3 2	1 2 4 3
		1 2 3 4

We can now analyze this composition as we did D_4. We begin first by letting $a = (1, 2)(3, 4)$ and $b = (2, 3)$ represent possible changes between rows. If we look at the first column of the Plain Bob Minimus composition, we see that it is nothing more than the dihedral group, D_4, which is a subgroup of S_4. To generate the second column of S_4 we introduce a $c = (3, 4)$ and we simplify our notation by letting $k = (ab)^3ac$. Multiplying through we generate the second column, $\{k, ka, kab, kaba, k(ab)^2, ka(ab)^2, k(ab)^3, k(ab)^3a\}$. Almost immediately we should realize that this is the left coset kD_4. Employing c again to obtain the third column yields k^2D_4, which is the final left coset since multiplication by c a third time brings us to rounds. The generation of the Plain Bob Minimus shows that S_4 can be expressed as the disjoint union of cosets of the subgroup D_4, that is, also stated, the cosets of D_4 in S_4 partition S_4. There is an important generalization of this fact, which states:

Theorem 111. *For any group G and any subgroup H, the cosets of H in G partition G.*

(See Exercise 5.9.5 above.)

Now, since we chose $a = (1, 2)(3, 4)$, $b = (2, 3)$, and $c = (3, 4)$, where b and c are obviously by definition 2-cycle or transpositions and a is the product of two such 2-cycles or transpositions, we have shown a further result, that each element of S_4 can be written as a product of 2-cycles. More generally, we can state the following theorem:

Theorem 112. *Let f be a member of S_n, i.e., let f be any permutation of degree n. Then f can be written as a product of transpositions.*

To sketch a proof of this theorem (following [G]) and hence prove Theorem 58 as promised, we need only to recall that: Every permutation of S_n can be written uniquely (up to order) as a product of disjoint cycles (Theorem 53 above).

Note that any cycle can be written as a product of transpositions as below:

$$(a_1, a_2, ..., a_k) = (a_1, a_k)(a_1, a_{k-1})...(a_1, a_2).$$

We see that since any permutation can be written in terms of cycles and any cycle can be written as product of transposition, it follows that every permutation of S_n can be written as a product of transpositions. □

Considering both the plain lead on four bells and the Plain Bob Minimus composition, it is obvious that group theory is latent in the study of campanology. As White concludes in his essay, he is not suggesting "that Fabian Stedman was using group theory explicitly, but rather that group theoretical ideas were implicit in (Stedman's) writings and compositions" ([Wh], p778). Whether we can consider Stedman the first group theorist, then, is unclear; what is clear, however, is that when we hear the bells of Westminster Abbey chime, we are hearing not just melody but mathematics.

Chapter 6

Graphs and "God's algorithm"

"...O, cursed spite,
that ever I was to set it right!"
Hamlet, Act 1, scene 5

In this chapter we introduce a graphical interpretation of a permutation group, the Cayley graph. This is then interpreted in the special case of a group arising from a permutation puzzle.

To begin, what's a graph? A graph is a pair of countable sets (V, E), where

- V is a countable set of singleton elements called vertices,
- E is a subset of unordered pairs $\{\{v_1, v_2\} \mid v_1, v_2 \in V\}$ called edges.

A graph is drawn by simply connecting points representing vertices together by a line segment if they belong to the same edge.

A digraph, or directed graph, is a pair of countable sets (V, E), where

- V is a countable set of vertices,
- E is a subset of ordered pairs $\{(v_1, v_2) \mid v_1, v_2 \in V\}$ called edges.

A digraph is drawn by simply connecting points representing vertices together by an arrow if they belong to the same edge (v_1, v_2), the araow originating at v_1 and arrowhead pointing to v_2.

If $e = \{v_1, v_2\}$ belongs to E then we say that e is an "edge from v_1 to v_2" (or from v_2 to v_1). If v and w are vertices, a path from v to w is a finite sequence of edges beginning at v and ending at w:

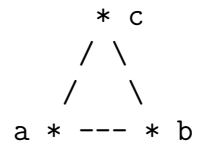
$$e_0 = \{v, v_1\}, e_1 = \{v_1, v_2\}, ..., e_n = \{v_n, w\}.$$

If there is a path from v to w then we say v is connected to w. We say that a graph (V, E) is connected if each pair of vertices is connected. The number of edges eminating from a vertex v is called the degree (or "valence") of v, denoted degree(v).

Example 113. : If

$$V = \{a, b, c\}, \quad E = \{\{a, b\}, \{a, c\}, \{b, c\}\},$$

then we may visualize (V, E) as



Each vertex has valence 2.

Definition 114. : If v and w are vertices connected to each other in a graph (V, E) then we define the distance from v to w, denoted $d(v, w)$, by

$$d(v, w) = \min_{v,w \in V \text{ connected}} \#\{\text{edges in a path from } v \text{ to } w\}$$

By convention, if v and w are not connected then we set $d(v, w) = \infty$. The diameter of a graph is the largest possible distance:

$$\text{diam}((V, E)) = \max_{v,w \in V} d(v, w).$$

In the above example, the diameter is 1.

6.1 Cayley graphs

Let G be a permutation group,

$$G =< g_1, g_2, ..., g_n > < \ S_X.$$

The Cayley graph of G with respect to $X = \{g_1, g_2, ..., g_n\}$ is the graph (V, E) whose vertices V are the elements of G and whose edges are determined by the following condition: if x and y belong to $V = G$ then there is an edge from x to y (or from y to x) if and only if $y = g_i * x$ or $x = g_i * y$, for some $i = 1, 2, ..., n$.

The Cayley digraph of G with respect to $X = \{g_1, g_2, ..., g_n\}$ is the digraph (V, E) whose vertices V are the elements of G and whose edges are determined by the following condition: if x and y belong to $V = G$ then there is an edge from x to y if and only if $y = x * g_i$, for some $i = 1, 2, ..., n$.

Exercise 6.1.1. Show that the Cayley graph of a permutation group is connected.

Lemma 115. *Let $\Gamma_G = (V, E)$ denote the Cayley graph associated to the permutation group $G =< g_1, g_2, ..., g_n >$. Let $N = |\{g_1, g_1^{-1}, g_2, g_2^{-1}, ..., g_n, g_n^{-1}\}|$. Then, for all $v \in V$,* degree$(v) = N$.

proof: Assume not. Then there is a $v \in V = G$ with either

(i) degree$(v) < N$, or

(ii) degree$(v) > N$.

First, we note that, for each $h \in \{g_1, g_1^{-1}, g_2, g_2^{-1}, ..., g_n, g_n^{-1}\}$, the set $\{v, h * v\}$ is an edge of Γ_G. This follows from the definition of the Cayley graph.

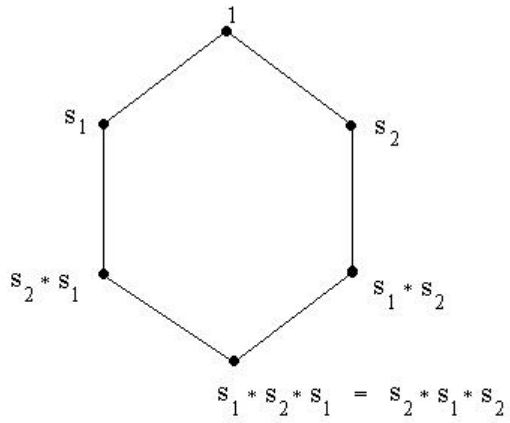
If $r =$ degree$(v) > N$ then, by definition of the Cayley graph, there are distinct $v_1, ..., v_r \in V$ with $v = h_i * v_i$, for all $1 \leq i \leq r$, where the $h_1, ..., h_r$ are distinct elements of $\{g_1, g_1^{-1}, g_2, g_2^{-1}, ..., g_n, g_n^{-1}\}$. This contradicts the definition of N.

If $r =$ degree$(v) < N$ then, by definition of the Cayley graph, there are distinct h_i, h_j in $\{g_1, g_1^{-1}, g_2, g_2^{-1}, ..., g_n, g_n^{-1}\}$ such that $h_i * v = h_j * v$. Since G is a group and $V = G$ (as sets), we may cancel the v's from both sides of the equation $h_i * v = h_j * v$, contradicting the assumption that h_i is distinct from h_j. □

Example 116. : Let

$$G =< s_1, s_2 >= S_3,$$

where $s_1 = (1\ 2)$, and $s_2 = (2\ 3)$. Then the Cayley graph of G with respect to $X = \{s_1, s_2\}$ may be visualized as

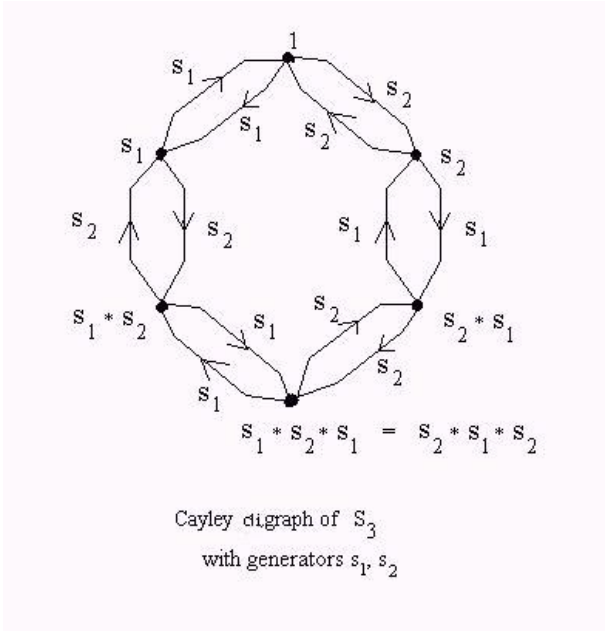


Cayley graph of S_3

Example 117. : Let

$$G =< s_1, s_2 >= S_3,$$

where $s_1 = (1\ 2)$, and $s_2 = (2\ 3)$. Then the Cayley digraph of G with respect to $X = \{s_1, s_2\}$ may be visualized as



Cayley digraph of S_3
with generators s_1, s_2

Exercise 6.1.2. Construct the Cayley graph of C_4, the cyclic group, with respect to the generator $s = (1, 2, 3, 4)$.

Exercise 6.1.3. Construct the Cayley graph of S_4, the symmetric group on four letters, with respect to the generators $s_1 = (1\ 2)$, $s_2 = (2\ 3)$ and $s_3 = (3\ 4)$.

Exercise 6.1.4. Construct the Cayley digraph of S_3 with respect to the generators $f = (1, 3)$, $r = (1, 2, 3)$. (Show, in particular, that f, r do indeed generate S_3.)

Example 118. : Let

$$G =< R, L, U, D, F, B > < S_{54}$$

be the group of the 3×3 Rubik's cube. Each position of the cube corresponds to an element of the group G (i.e., the move you had to make to get to that position). In other words, each position of the cube corresponds to a vertex of the Cayley graph. Each vertex of this graph has valence 12

Exercise 6.1.5. Check this.

Moreover, a solution of the Rubik's cube is simply a path in the graph from the vertex associated to the present position of the cube to the vertex associated to the identity element. The number of moves in the shortest possible solution is simply the distance from the vertex associated to the present position of the cube to the vertex associated to the identity element. The diameter of the Cayley graph of G is the number of moves in the best possible solution in the worst possible case.

6.2 God's algorithm

Problem: Let G be the group of a permutation puzzle. Find the diameter of the Cayley graph of G.

This problem is unsolved for must puzzles (including the 3×3 Rubik's cube) and appears to be very difficult computationally. The cases where it is known include (with no attempt at completeness) the following:

puzzle	diameter
pyraminx	11 (not including tip moves)
2×2 Rubik's cube	14

For the 2×2 Rubik's cube, see [CFS].

Problem: Let G be the group of a permutation puzzle and let v be a vertex in the Cayley graph of G. Find an algorithm for determining a path from v to the vertex v_0 associated to the identity having length equal to the distance from v to v_0.

This problem is much harder. The algorithm, if it exists, is called God's algorithm. A good reference for recent progress on God's algorithm for various Rubik's cube-like puzzles may be found on Mark Longridge's www page [Lo].

Exercise 6.2.1. Find the Cayley graph of the "sliced squared" group

$$G =< M_R^2, M_F^2, M_D^2 >,$$

where M_R is the middle slice move which turns the middle slice parallel to the right face clockwise 90 degrees (with respect to the right face). Find the diameter of this graph.

Let Γ be a graph. A Hamiltonian circuit on Γ is a sequence of edges forming a path in Γ which passes through each vertex exactly once. (If you think of the vertices as cities and the edges as roads then a Hamiltonian circuit is a tour visiting each city exactly once.)

The following unsolved problem was first mentioned in this context (as far as I know) by A. Schwenk:

Problem: Let G be the group of the 3×3 Rubik's cube puzzle. Does the Cayley graph of G have a Hamiltonian circuit? In other words, can we (in principle) "visit" each possible position of the Rubik's cube exactly once, by making one move at a time using only the basic generators R, L, U, D, F, B?

This is a special case of a more general unsolved problem: For an arbitary permutation group with more than two elements, it is not known if the Cayley graph is Hamiltonian [CG].

An example of one where it is known is the following:

Example 119. Let G be the group S_n with generators given to be the set of all transpositions:

$$G = S_n, \qquad X = \{(i, j) \mid 1 \leq i < j \leq n\}.$$

(There are many more transpositions than necessary to generate S_n since the subset of transpositions of the form $(i, i+1)$, $1 \leq i \leq n-1$, suffice to generate S_n [R].) The algorithm of Steinhaus (see §3.3) shows that there is a Hamiltonian circuit in the Cayley graph of S_n with respect to X.

The reader interested in more examples is referred to [CG].

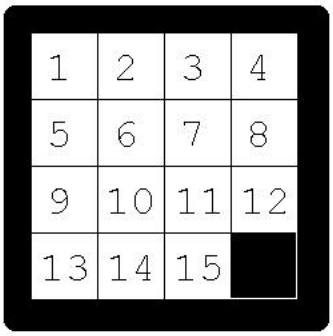
6.2.1 The Icosian game

Sir William Hamilton, an Irish prodigy of the 18th century, may have originated the problem of finding Hamiltonian paths (hence the name) by patenting a game called the Icosian game or the Hamilton game. The idea is to find a Hamiltonian path around the vertices of the icosahedron. A picture (from the MacTutor History of Mathematics archive [OR]) of the orginal game is:

6.3 The graph of the 15 puzzle

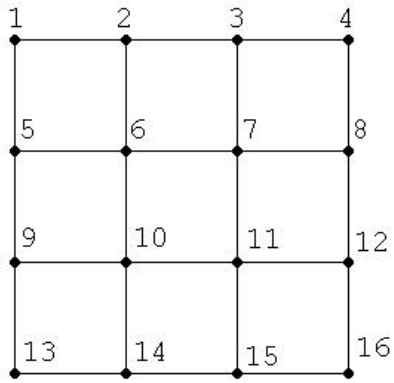
This section, which is based on [Mc], discusses the 15 puzzle from the graph-theoretical point of view following [W].

The 15 puzzle was introduced in §4.1 above. The object of the puzzle was to order the pieces from one to fifteen from left to right, top to bottom, as shown in the solved position:



To solve a mixed up puzzle, one would slide the squares around in the puzzle. In order to do this you must slide a numbered square into the place of the space. We could represent this mathematically by saying that this is a transposition of that numbered square and the blank.

If we label each space in the puzzle in the above Figure, as a vertex, and label the vertices numerically, then the resulting graph is represented by

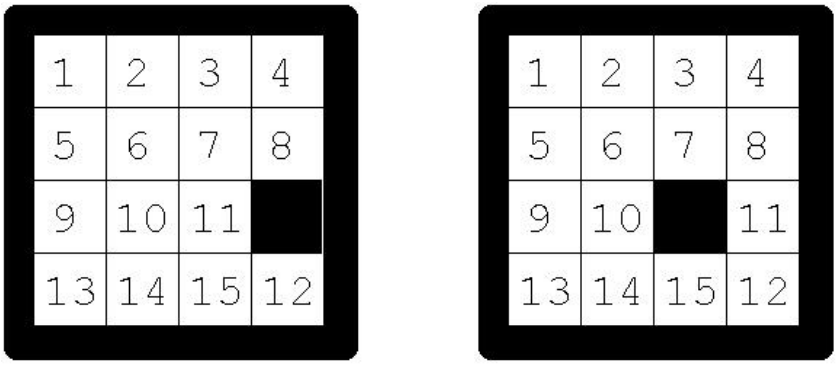


We will let 16 denote the blank and call this graph Γ. The only legal moves of the puzzle are transpositions of the 16th vertex and a vertex that is adjacent to it. Therefore, any permutation of the vertices produces a labeling on Γ.

6.3.1 General definitions

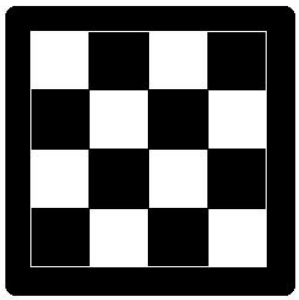
Now let Γ be a simple graph with the vertex set $V(\Gamma)$ of cardinality N. (In the above example $N = 16$.) By a labeling we mean the placement of the numbers one through N on distinct vertices of Γ, where N denotes the blank. In other words, a labeling on Γ is a bijective mapping $f : V(\Gamma) \to \{1, 2, ..., N\}$. Two labelings f, g on Γ are adjacent if and only if g is a result of a single transposition on f of vertex N with a vertex adjacent to N on f. In other words, f and g are adjacent if they differ by one legal move of the puzzle. From Γ, we make a new graph $puz(\Gamma)$ as follows [W]: the vertex set $V(puz(\Gamma))$ contains all labelings on Γ, and two vertices in $puz(\Gamma)$ are joined by an edge if the associated labelings are adjacent.

For example, the labelings below are adjacent:



We can consider a sequence of moves on Γ to be a path p, such that $p = (x_0, x_1, x_2, ..., x_n)$ where the $x_i's$ are vertices of Γ, and x_i and x_{i-1} are adjacent. Such a path p is said to be from x_0 (its initial vertex) to x_n (its terminal vertex). The path p is simple if $x_0, x_1, x_2, ..., x_n$ are distinct. If $x_0 = x_n$ then (a not necessarily simple path) p is called a closed path based at x_0. Let x_0 be a fixed vertex of Γ. The set of paths based at x_0 forms a group (under composition of paths) called the homotopy group of Γ based at x_0, denoted $\Gamma(x_0)$.

Now suppose we paint the blocks of the 14-15 puzzle in a checkerboard pattern:



In this arrangement the blank would start on a white square. If we were to move the blank up, then it is now on a black square. That is one transposition, therefore the movement is odd. If we then move the blank to the left, the blank would be on a white square. This is a total of two transpositions; therefore, the movement is even. After three transpositions the blank would be on a black square, therefore it would be an odd permutation. Therefore if the blank ends on a white square, an even permutation has occurred. If the blank ends on a black square, an odd permutation has occurred.

A legal position of the 15-Puzzle is any sequence of legal transpositions starting from the solved position such that the blank ends up in the bottom right-hand corner. Each such position corresponds to a permutation of the 15 numbered vertices and hence to an element of the symmetric group S_{15}. The set of all such permutations (arising as a sequence of transpositions) in S_{15} forms a group called the group of the 15-Puzzle.

Note that the group of the 15-puzzle is isomorphic to the homotopy group of the 15 puzzle graph based at the "blank" vertex.

If we assign the number 16 to the blank, then we can see that we can arrange the pieces of the puzzle in 16! different ways. However, if we take only legal positions of the 15-Puzzle, then we are fixing one of the pieces. As a result the number of ways to permute the rest of the pieces, with the blank on the white square at the bottom right-hand corner, is at most 15!. All such permutations have to be even, by the checkerboard analysis above. 15!/2 is the number of even permutations of 15 elements (there are an equal number of even and odd permutations). From this we see that the 15-puzzle has 15!/2 possible legal positions.

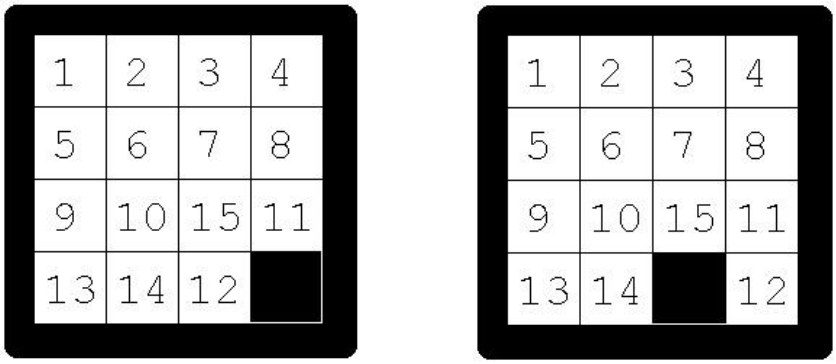
Theorem 120. *The positions with the empty space at the bottom right that can be reached from the start position of the 15-Puzzle by shifting tiles are in*

a bijective correspondence with the $15!/2 = 1,307,674,368,000$ *even permutations of the numbers from 1 to 15.*

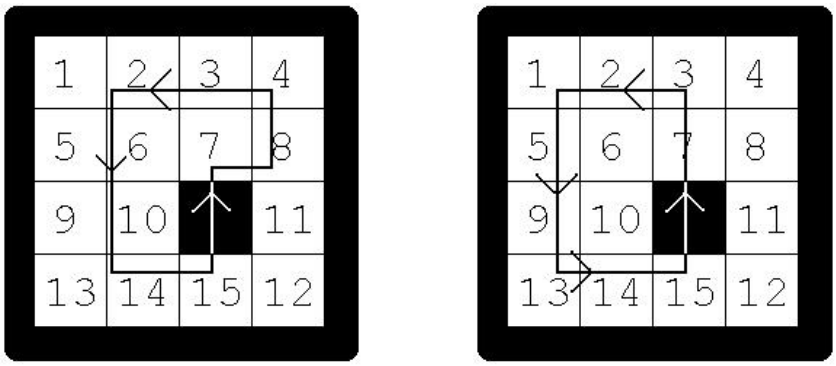
Remark 9. The 14-15 Puzzle cannot be solved, because it is an odd permutation. It only has one transposition, 14 interchanged with 15.

proof: If we label the empty space 16, then every possible position of the puzzle may be regarded as an element of the symmetric group S_{16} and an element of $puz(\Gamma)$. There are 16! elements in S_{16}, and 16! vertices of $puz(\Gamma)$. With the argument earlier we can show that all legal positions of the puzzle are obtained by an even number of transpositions. Therefore, all legal moves are even permutations of the puzzle.

Now we must show that there is a certain 3-cycle in the group of the 15-Puzzle. For example, if we shift the three pieces surrounding the empty space around in a circle following the order of moves south-east-north-west then the three-cycle (11, 12, 15) is produced, as indicated in the previous Figures combined with



It can be shown that if you fix the 11 and 12 pieces, then any other piece can take the place of the 15 by following one of the cycles below:



By Lemma 160, such 3-cycles generate A_{15}. This proves the theorem.

Alternatively, with some work we can show that any number can replace the 11 in the three-cycle, and we can show that any other number can replace the 12. From this we can conclude that any three-cycle can be formed. Since every even permutation is a combination of three-cycles (by Proposition 159), every even permutation of the 15-Puzzle can be reached. □

With this information, we can make a generalization to rectangular puzzles of size $m \times n$ with $m > 1$ and $n > 1$:

Theorem 121. *The group of an $m \times n$ rectangular puzzle is the alternating group A_{mn-1}.*

The proof of this is similar to the proof for the 4×4 puzzle, if $m > 3$ and $n > 3$. (The special cases when $1 < m < 4$ or $1 < n < 4$ must be treated separately). The size of the alternating group is given by $(mn - 1)!/2$.

6.4 Remarks on applications, NP-completeness

Cayley graphs have been used by computer scientists to model interconnection networks for parallel processors (see [CFS], [CG] for some references).

The problem of finding an efficient algorithm for the shortest solution to the $m \times n$ puzzle is difficult. It amounts to finding the shortest path between two points in a graph which is, in general, a difficult problem computationally [GJ].

There is a class of problems called "NP-complete" problems. Without getting into precise details which would take us too far afield, this is a class of problems which are in some sense "equally hard" to solve. If you can find a "polynomial time" algorithm to solve one then you can find one to solve any other problem in that class as well. For example, [GJ] and [BCG] have a list of games and puzzles whose solutions are NP-complete problems.

Chapter 7

Symmetry groups of the Platonic solids

> "Plato said God geometrizes continually."
> *Plutarch*
> *Convivialium disputationum, liber 8,2*

> "We do not listen with the best regard to the verses of a man who is only a poet, nor to his problems if he is only an algebraist; but if a man is at once acquainted with the geometric foundation of things and with their festal splendor, his poetry is exact and his arithmetic musical."
> *Ralph Waldo Emerson*
> *Society and Solitude*
> *chapter 7, Work and Days*

This chapter requires a little more mathematical sophistication from the reader than the earlier chapters. However, the exercises are (I think) choosen to be doable.

7.1 Descriptions

The "Platonic solids" are the 5 regular polyhedrons:

polyhedron	# faces	# vertices	# edges	group	p,q
tetrahedron	4	4	6	T	3,3
hexahedron	6	8	12	O	4,3
octahedron	8	6	12	O	3,4
dodecahedron	12	20	30	I	5,3
icosahedron	20	12	30	I	3,5

Here:

p, called the face degree, denotes the number of edges bounding each face,

q, called the vertex degree, denotes the number of faces meeting each vertex.

A vertex of one of these solids is therefore specified by the q-tuple of faces meeting that vertex. We saw several examples of this already when we specified notation for the movements of the associated Rubik's cube-like puzzles in chapter 5.

These solids may be drawn in rectangular coordinates using

polyhedron	coordinates
tetrahedron	(1,1,1), (1,-1,-1), (-1,-1,1), (-1,1,-1)
hexahedron	(1,1,1), (1,1,-1), (1,-1,1), (-1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1), (-1,-1,-1)
octahedron	(1,0,0), (0,0,1), (0,1,0), (-1,0,0), (0,-1,0), (0,0,-1)
dodecahedron	$(0,\pm\phi^{-1},\pm\phi)$, $(\pm\phi^{-1},\pm\phi,0)$, $(\pm\phi,0,\pm\phi^{-1})$, $(\pm1,\pm1,\pm1)$,
icosahedron	$(1,0,\phi)$, $(1,0,-\phi)$, $(-1,0,\phi)$, $(-1,0,-\phi)$, $(0,\phi,1)$, $(0,\phi,-1)$, $(0,-\phi,1)$, $(0,-\phi,-1)$, $(\phi,1,0)$, $(\phi,-1,0)$, $(-\phi,1,0)$, $(-\phi,-1,0)$

where ϕ denotes the golden ratio.

If P_1, P_2, P_3 are three vertices of an icosahedron which form a triangular face then $(P_1+P_2+P_3)/3$ forms a vertex of the dual dodecahedron and every vertex of the dual dodecahedron arises in this way.

The three "Platonic groups" (the group of "symmetries" of these figures) will be described below. Their names:

T = symmetric group of the tetrahedron = tetrahedral group,

O = symmetric group of the octahedron (or cube) = octahedral group,

I = symmetric group of the icosahedron (or dodecahedron) = icosahedral group.

7.2 Background on symmetries in 3-space

This subsection presents, with some proofs, background on isometries in 3 dimensions necessary for understanding the symmetry groups of the Platonic solids.

We fix once and for all the "right-hand-rule" orientation in 3-space. We call a distance-preserving transformation in 3-space which fixes the origin a symmetry of 3-space. We say that such a symmetry is orientation preserving if it preserves the right-hand rule orientation.

Example 122. : Let $s : \mathbb{R}^3 \to \mathbb{R}^3$ denote the function which takes each vector v belonging to $\mathbb{R}^3$ and returns its reflection $s(v)$ about the yz-plane. This is not orientation preserving since it reverses the direction of a counterclockwise moving circular path in the yz-plane. In terms of rectangular coordinates, $s(x, y, z) = (-x, y, z)$.

Let

$$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \text{ real numbers}\}$$

denote 3-space. We also write this, when convenient, as column vectors

$$\mathbb{R}^3 = \{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mid x, y, z \text{ real}\}$$

The distance function on $\mathbb{R}^3$ is the function

$$d(\vec{v}_1, \vec{v}_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

where $\vec{v}_1 = (x_1, y_1, z_1)$, $\vec{v}_2 = (x_2, y_2, z_2)$. This may be expressed in terms of the inner product $\vec{v}_1 \cdot \vec{v}_2 = x_1x_2 + y_1y_2 + z_1z_2$ as $d(\vec{v}_1, \vec{v}_2) = \sqrt{(\vec{v}_1 - \vec{v}_2) \cdot (\vec{v}_1 - \vec{v}_2)}$. Conversely, the polarization identity:

$$\vec{v}_1 \cdot \vec{v}_2 = \frac{1}{2}(||\vec{v}_1 + \vec{v}_2||^2 + ||\vec{v}_1 - \vec{v}_2||^2)$$

allows one to recover the value of the inner product from the knowledge of the values of the distance function.

We call a function $f : \mathbb{R}^3 \to \mathbb{R}^3$ an isometry if it satisfies

$$d(f(v_1), f(v_2)) = d(v_1, v_2)$$

for all v_1 and v_2 belonging to $\mathbb{R}^3$.

We want to understand isometries a little better since they will preserve distances (and, in particular, preserve the shapes of solids) and therefore provide us with the kinds of symmetries of 3-space we want to consider. We can construct isometries using certain types of 3×3 matrices. (Appendix 1 of this chapter gives a little background on matrices.)

Lemma 123. *If A is a 3×3 matrix then the function $A : \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry if and only if $A^t * A = I_3$, where A^t denotes the transpose identity matrix (obatined by flipping the entries of A about the diagonal.*

Remark 10. In particular, if A is an isometry then $\det(A)^2 = \det(A^t)\det(A) = \det(A^t * A) = \det(I_3) = 1$.

proof: The distance function is preserved if and only if the dot product function is preserved. (This is a consequence of the "polarization identity" - see the appendix.) Let $m(\vec{v}, \vec{w}) = \vec{v} \cdot \vec{w}$, where $\cdot$ denotes the vector dot product. Since $m(A\vec{v}, B\vec{w}) = \vec{v} \cdot (A^t * B)\vec{w}$, we have

$$m(A\vec{v}, A\vec{w}) = m(\vec{v}, \vec{w}), \qquad \forall v, w \in \mathbb{R}^3$$

if and only if

$$\vec{v} \cdot (A^t * B)\vec{w} = \vec{v} \cdot \vec{w}, \qquad \forall v, w \in \mathbb{R}^3$$

if an only if $A^t * A = I_3$. $\square$

You may have been wondering how one could construct an isometry. This lemma gives us lots of examples.

Example 124. A rotation matrix in 3-dimensions may be written in the form

$$R(\phi, \theta, \psi) = \begin{pmatrix} r_{11} & r_{12} & \sin(\theta)\sin(\psi) \\ r_{21} & r_{22} & \sin(\theta)\cos(\psi) \\ \sin(\phi)\sin(\theta) & -\sin(\theta)\cos(\phi) & \cos(\theta), \end{pmatrix}$$

where

$$\begin{aligned} r_{11} &= \cos(\phi)\cos(\psi) - \cos(\theta)\sin(\phi)\sin(\psi), \\ r_{12} &= \sin(\phi)\cos(\psi) + \cos(\theta)\cos(\phi)\sin(\psi), \\ r_{21} &= -\cos(\phi)\sin(\psi) - \cos(\theta)\sin(\phi)\cos(\psi), \\ r_{22} &= -\sin(\phi)\sin(\psi) + \cos(\theta)\cos(\phi)\cos(\psi). \end{aligned}$$

and where the angles ϕ, θ, ψ are the "Euler angles". This represents the rotation of 3-space obtained by the following sequence of rotations: rotate by angle ψ about the z-axis, rotate by the angle θ about the x-axis ($0 \leq \theta \leq \pi$), then rotate by angle ϕ about the z-axis again.

Although this is an interesting fact due to its explicitness, we shall not use this expression.

Question: Are there any isometries which do not come from matrices as in the above lemma? Yes: any translation gives rise to an isometry.

Question: Are there any examples of isometries which do not arise from a composition of a translation and an orthogonal matrix? No: the following theorem classifies all the isometries.

Theorem 125. *A function $f : \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry fixing the origin if and only if f is left multiplication by an orthogonal matrix.*

This will not be proven here (see Artin [Ar], chapter 4, section 5, Proposition 5.16).

As a consequence of this lemma, we see that if the matrix A gives rise to as isometry then $\det(A)$ is either equal to 1 or -1 (since $det(A)^2 = det(A^t * A) = det(I_3) = 1$). In particular, the determinant of such a matrix is non-zero, so the matrix is invertible.

Lemma 126. *The set of all 3×3 matrices A such that the function $A : \mathbb{R}^3 \to \mathbb{R}^3$ is an isometry forms a group under matrix multiplication.*

Exercise 7.2.1. Verify the group axioms needed to prove this lemma.

Notation: This group will be denoted $O_3(\mathbb{R})$ and called the orthogonal group of $\mathbb{R}^3$. We denote by $SO_3(\mathbb{R})$ the following subset

$$SO_3(\mathbb{R}) = \{A \in O_3(\mathbb{R}) \mid det(A) = 1\}.$$

which is called the special orthogonal group of $\mathbb{R}^3$.

Lemma 127. *$SO_3(\mathbb{R})$ is a subgroup of $O_3(\mathbb{R})$.*

Exercise 7.2.2. Verify the group axioms for $SO_3(\mathbb{R})$.

It is known that the number of cosets in $O_3(\mathbb{R})/SO_3(\mathbb{R})$ is 2. In fact, it is known that

$$O_3(\mathbb{R}) = SO_3(\mathbb{R}) \cup s * SO_3(\mathbb{R}) \quad \text{(disjoint union)} \tag{7.1}$$

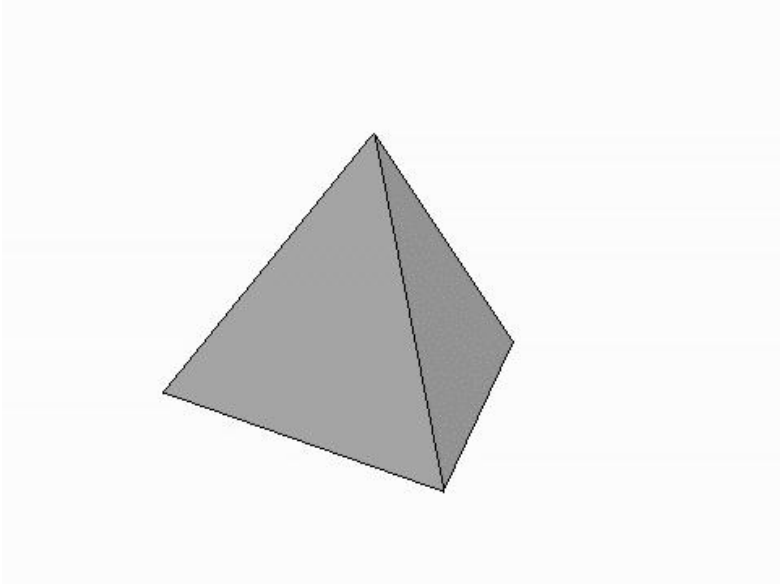
where s is the reflection in the above example (this follows from [Ar], chapter 4, section 5).

Lemma 128. *The isometry A in $O_3(\mathbb{R})$ is orientation preserving if and only if $det(A) = 1$.*

We will not prove this lemma here.

7.3 Symmetries of the tetrahedron

Fix a tetrahedron centered at the origin, with one vertex along the z-axis. Each edge has an "opposite" edge on the tetrahedron (which is actually perpendicular to it if you look at it straight on). Each vertex has an "opposite" face.



There are orientation preserving symmetries (called rotations) of the tetrahedron and orientation reversing symmetries of the tetrahedron. The orientation preserving symmetries of the tetrahedron will be denoted ST. They are obtained as follows:

- the 4 axes of symmetry through the centers of the faces yield 2 elements each (120 degree clockwise rotation when viewed from outside and a 240 degree rotation), for a total of 8 elements,

  (This "tetrahedral symmetry" allows for the mechanical construction of the pyraminx.)

- the 3 pairs of edges (formed by an edge and its opposite) yield one element each (a 180 degree rotation), for a total of 3 elements.

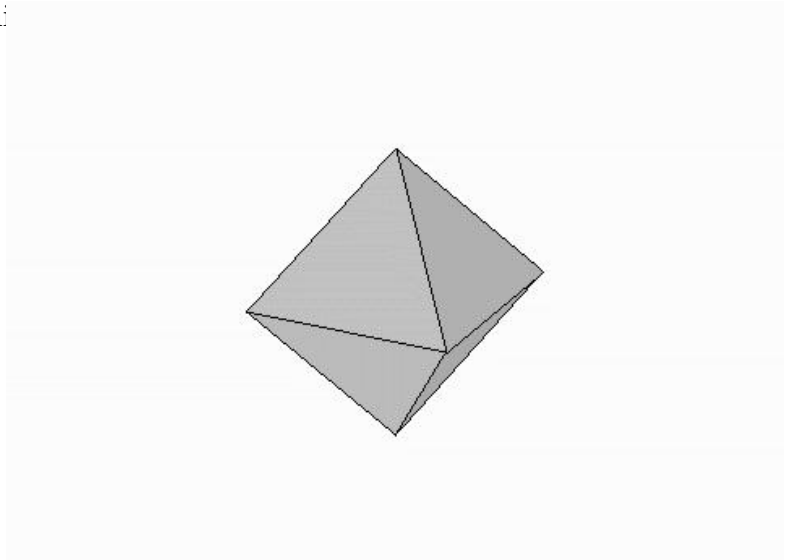
These, plus the identity, give 12 elements in ST.

Using the coset decomposition (7.1), we have $T = ST \cup s * ST$ (disjoint), so $|T| = 24$.

Remark 11. It turns out that ST is essentially the alternating group A_4 of even permutations of S_4 and T is essentially S_4 itself. We shall state the precise result in the next chapter.

7.4 Symmetries of the cube

We fix a cube centered about the origin in 3-space. The set of centers of the faces of a cube forms a set of vertices of an octahedron drawn inside the cube. Th



These two polyhedra have the same symmetry group, which we denote by O. There are orientation preserving symmetries, or rotations, of the cube and orientation reversing symmetries of the cube. The orientation preserving symmetries of the cube will be denotes SO. They are obtained as follows:

- the 3 axes of symmetry through the centers of the faces yield 3 elements each (90 degree clockwise rotation when viewed from outside, a 180 degree rotation, and a 270 degree rotation), for a total of 9 elements,

  (This "hexahedral symmetry" allows for the mechanical construction of the Rubik's cube.)

- the 4 axes through the opposing vertices yield 2 elements each (all of order 3), for a total of 8 elements,

  (This "tetrahedral symmetry" allows for the construction of the skewb [H].)

- the 6 axes through the opposing mid-edge points yield 1 element each (of order 2), for a total of 6 elements.

These elements, plus the identity, yield 24 elements.

Lemma 129. *There are 24 orientation preserving elements in O, i.e., $|SO| = 24$.*

The above sketch is one way to see why this is true. Here's another

proof: Let V be the set of vertices of the cube. The group SO acts on the set V. Fix a v belonging to V and let $H = stab_{SO}(v)$. One can check that $|H| = 3$ (since the only symmetry which fixes v is a rotation g about the line through v and its opposite vertex. Since g is order 3, $H =< g >$ is order 3 as well). We have $|V| = 8$, so by a lemma in the previous chapter on orbits and stabilizers, we have $|SO/H| = |V|$. By Lagrange's theorem, $|SO| = |SO/H||H| = 8 \cdot 3 = 24$. $\square$

Now we know SO, what is O? Note that s, the reflection in the example in the previous section, belongs to O. Using the coset decomposition of the previous section, we have the coset decomposition

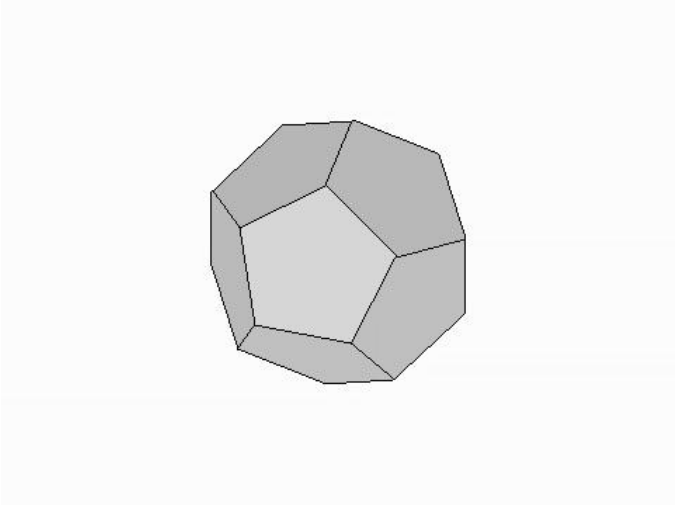
$$O = SO \cup s * SO \qquad \text{(disjoint union)}.$$

We know that $|s * SO| = |SO| = 24$, so

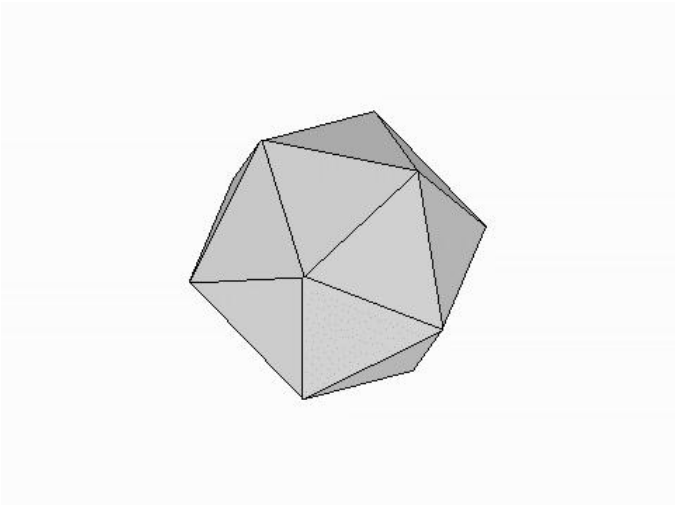
Lemma 130. *The order of the octahedral group is $|O| = 48$.*

Remark 12. It turns out that SO is essentially the symmetric group S_4 and O is "isomorphic to the direct product" $S_4 \times C_2$. We shall state the precise definitions and result in the next chapter.

7.5 Symmetries of the dodecahedron



The set of centers of the faces of a dodecahedron forms a set of vertices of an icosahedron drawn inside. This icosahedron is called the "dual" polyhedron. We fix a dodecahedron in 3-space so that the vertices of the dual icosahedron are as listed in section 1 above.



Let SI denote the group of orientation preserving symmetries of the dodecahedron. Note SI is a finite subgroup of $SO_3(\mathbb{R})$. Let I denote the

group of all symmetries of the dodecahedron. Note I is a finite subgroup of $O_3(\mathbb{R})$ and that SI is a subgroup of I. Let F denote the set of faces of the dodecahedron, so $|F| = 12$. SI acts on F.

Lemma 131. *SI acts on F transitively.*

We won't prove this. If you look at a dodecahedron it follows "by inspection". The reason why this is useful is that it tells us that if x is any face then any other face can be obtained from x by applying some element of SI. In other words, the orbit of x is all of F: $SI * x = F$.

If x is any face then the only orientation preserving symmetries which don't send x to a different face is a rotation by an integer multiple of 72 degrees about the line passing through the center of x and the center of its opposite face. There are, for each face x, exactly 5 distinct rotations of this type. Therefore,

$$|stab_{SI}(x)| = 5.$$

By a lemma in the section on orbits, we have

$$SI/stab_{SI}(x) = SI * x,$$

so $|SI| = |stab_{SI}(x)||SI * x| = 5 \cdot 12 = 60$.

The elements of SI include:

- rotation by $2 * \pi * k/5$, $k = 0, 1, 2, 3, 4$, about the line passing through the center of a face and its opposite,

  (This "dodecahedral symmetry" allows for the construction of the megaminx.)

- rotation by $2 * \pi * k/3$, $k = 0, 1, 2$, about the line passing through a vertex and its opposite,

- rotation by π about the center of an edge.

Subgroups include:

- stabilizer of a vertex. These are all cyclic of order 3, and they are all conjugate. There are 10 distinct such subgroups since a vertex and its opposite share the same stabilizer.

- stabilizer of a face. These are all cyclic of order 5, and they are all conjugate. There are 6 distinct such subgroups since a face and its opposite share the same stabilizer.

- stabilizer of an edge. These are all cyclic of order 2, and they are all conjugate. There are 15 distinct such subgroups.

Exercise 7.5.1. Verify all these.

Remark 13. It turns out that SI is essentially the alternating group A_5 of even permutations of S_5 and I is "isomorphic to the direct product" $A_5 \times S_5$. We shall state the precise result in the next chapter.

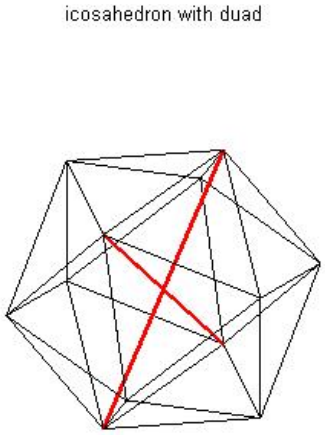
For an excellent discussion of the symmetries of the icosahedron, see [Ba].

7.6 Appendix: Symmetries of the icosahedron and S_6

A duad is a pair of diagonals (a diagonal is a segment from a vertex to its antipodal opposite vertex) of the icosahedron. The top of the icosahedron has 6 vertices and each diagonal must have exactly one of these 6 vertices as an endpoint. There are 12 vertices, hence 6 diagonals, hence

$$\begin{pmatrix} 6 \\ 2 \end{pmatrix} = 15$$

different duads. Each duad determines a "golden rectangle" (i.e., a rectangle whose ratio length/width is either the golden ratio $\phi = (1 + \sqrt{5})/2$ or its inverse. We may identify a duad with a pair of distinct integers $\{(i, j) \mid 1 \leq i < j \leq 6\}$, i.e., with a 2-cycle in S_6. A duad may be pictured as



Each element of the rotation group of the icosahedron (i.e., the group of orientation-preserving symmetries of the icosahedron) must send a duad to a duad. Each duad has 4-fold symmetry, i.e., can be send to itself in 4 ways. There are 15 duads, so there are $4 \cdot 15 = 60$ ways to send a duad to another. This is precisely the number of orientation-preserving symmetries of the icosahedron.

The 18-th century mathematician Sylvester (who, though from Great Britain, once taught in Maryland) called a partitioning

$$X = X_1 \cup ... \cup X_n \qquad \text{(disjoint)},$$

of a set X a syntheme if each of the sets $X_i, 1 \leq i \leq n$, has the same number of elements. If we take

$$X = \{\text{set of diagonals of the icosahedron}\}$$

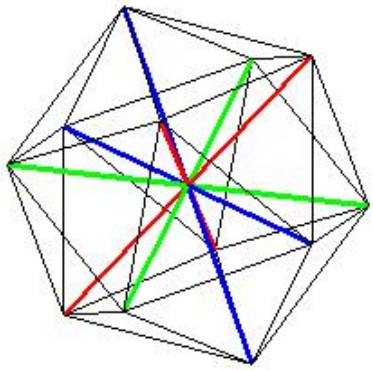
then a syntheme is a set of three duads, no two having a diagonal in common. There are

$$\left(\begin{array}{c} 6 \\ 2 \end{array} \right) \left(\begin{array}{c} 4 \\ 2 \end{array} \right) /3! = 15$$

different synthemes (the 3! since there are 3! ways to permute the duads amongst themselves). A syntheme may be represented by a coloring of the vertices on the top of the icosahedron using three colors, each for exactly two

vertices. We may identify a syntheme with a product of 3 distinct 2-cycles in S_6. A syntheme may be pictured as

icosahedron with true cross syntheme



We partition the set of 15 duads into 5 groups of 3 as follows. (Recall each syntheme is a triple of duads.) First, pick a syntheme, A_1. Pick another syntheme A_2, so that A_1, A_2 have no duad in common. Continue on in this way until you pick five synthemes $A_1, .., A_5$, no two of which have a duad in common. Such a choice of 5 synthemes is called a pentad. There a 6 pentads, which we label $P_1, ..., P_6$ in any way you like. (A list of the six pentads is given in [R], chapter 7.) Any permutation of the 6 diagonals of the icosahedron gives rise to a permutation of the set of 6 pentads. Hence any permutation of the 6 diagonals of the icosahedron, which may be regarded as an element of S_6, gives rise to a permutation of the set of 6 pentads, which may also be regarded as an element of S_6. This gives a map

$$f : S_6 \to S_6.$$

This example will be discussed further in the next chapter. See also [R] and [Ba].

Chapter 8

Groups, II

"The art of doing mathematics consists in finding that special case which contains all the germs of generality."
David Hilbert

Groups are analogous to molecules. We (mathematicians) want to know what they "look like", we want to know how to describe them, how to compare them, how to "make" more of them, if they fall into "families" with similar properties...

Given two groups G_1, G_2, a natural question is to ask how "similar" are they? (Exactly what is meant by "similar" will be explained later.) We shall, in this chapter, introduce notions and techniques useful for comparing two groups. In a later chapter, we will focus on the 3×3 Rubik's cube group by comparing it to "better understood" groups.

8.1 Homomorphisms

A homomorphism between two groups is, roughly speaking, a function between them which preserves the (respective) group operations.

Definition 132. Let G_1, G_2 be groups, with $*_1$ denoting the group operation for G_1 and $*_2$ the group operation for G_2. A function $f : G_1 \to G_2$ is a homomorphism if and only if, for all $a, b \in G_1$, we have

$$f(a *_1 b) = f(a) *_2 f(b).$$

Exercise 8.1.1. Prove the following: If $f : G_1 \to G_2$ is a homomorphism of groups then

$$f(G_1) = \{g \in G_2 \mid g = f(x), \text{ for some } x \in G_1\}$$

is a subgroup of G_2.

The subgroup $f(G_1) < G_2$ is called the image of f and is sometimes denoted $im(f)$.

Example 133. Let G be a group and h a fixed element of G. Define $f : G \to G$ by

$$f(g) = h^{-1} * g * h, \quad g \in G.$$

Then the following simple trick

$$f(a * b) = h^{-1} * (a * b) * h = h^{-1} * a * h * h^{-1} * b * h = f(a) * f(b)$$

shows that f is a homomorphism. In this case, $im(f) = G$, i.e., f is surjective.

Exercise 8.1.2. Let

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Now, let $G =< A, B >$ denote the group of all matrices which can be written as any arbitrary product of these two matrices (in any order and with as many terms as you want). We have

$$G = \{I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\}$$

(You may want to try to check this as an exercise by regarding each such matrix as a permutation matrix.) Define $f : G \to S_3$ by

g	$f(g)$
I_3	1
A	s_1
B	s_2
$A * B$	$s_1 * s_2$
$B * A$	$s_2 * s_1$
$A * B * A$	$s_1 * s_2 * s_1$

Show that this is a homomorphism.

Example 134. The function

$$sgn : S_n \to \{\pm 1\},$$

which assigns to each permutation its sign, is a homomorphism. One reason why this is true is because the sign of a permutation g is the determinant of the associated permutation matrix $P(g)$. Since the determinant of the product is the product of the determinants (this is a basic result in linear algebra [JN]), we have $sgn(gh) = \det P(gh) = \det P(g) \det P(h) = sgn(g)sgn(h)$, for all $g, h \in S_n$. From this it follows that sgn is a homomorphism.

Lemma 135. *If $f : G_1 \to G_2$ is a homomorphism then*

(a) $f(e_1) = e_2$, where e_1 denotes the identity element of G_1 and e_2 denotes the identity element of G_2,

(b) $f(x^{-1}) = f(x)^{-1}$, for all x belonging to G_1,

(c) $f(y^{-1} *_1 x *_1 y) = f(y)^{-1} *_2 f(x) *_2 f(y)$, for all x, y belonging to G_1, ($*_1$ denoting the group operation for G_1 and $*_2$ the group operation for G_2).

proof: (a) We have $f(x) = f(x *_1 e_1) = f(x) *_2 f(e_1)$, for any $x \in G_1$. Multiply both sides of this equation on the left by $f(x)^{-1}$.

(b) We have, by part (a), $e_2 = f(e_1) = f(x *_1 x^{-1}) = f(x) *_2 f(x^{-1})$. Multiply both sides of this equation on the left by $f(x)^{-1}$.

Exercise 8.1.3. Prove part (c).

□

Definition 136. Let G_1, G_2 be finite groups. We say that G_1 embeds (or injects) into G_2 if there exists an injective homomorphism $f : G_1 \to G_2$. A homomorphism $f : G_1 \to G_2$ is a isomorphism if it is a bijection (as a function between sets). In this case, we call G_1 and G_2 isomorphic and write $G_1 \cong G_2$. An isomorphism from a group G to itself is called an automorphism.

The notion of an isomorphism is the notion we will use when we want to same two groups are "essentially the same group", i.e., one is basically a carbon copy of the other with the elements relabeled.

8.2 Homomorphisms arising from group actions

Lemma 137. *Let G be a group and X a finite set. If G acts on X (on the left, resp. on the right) then there is a homomorphism $G \to S_X$ given by $g \longmapsto \phi_g$. Conversely, if $\phi : G \to S_X$ is a homomorphism then $\phi(g) : X \to X$ defines a (left, resp. right) action of G on X.*

Exercise 8.2.1. Prove this.

Example 138. Let G be the Rubik's cube group generated by the basic moves R, L, U, D, F, B. For each move $g \in G$, let $\rho(g)$ be the corresponding permutation of the set of vertices V of the cube and let $\sigma(g)$ be the corresponding permutation of the set of edges E of the cube. Let S_n denote the symmetric group on n letters and identify S_V with S_8, S_E with S_{12}. Then

(a) $\rho : G \to S_8$ is a homomorphism,

(b) $\sigma : G \to S_{12}$ is a homomorphism.

Exercise 8.2.2. Prove this.

Definition 139. Let G act on a set X. We call the action k-tuply transitive if for each pair of ordered k-tuples $(x_1, x_2, .., x_k), (y_1, y_2, .., y_k)$ of elements belonging to X there is a $g \in G$ such that $y_i = \phi_g(x_i)$ for each $1 \leq i \leq k$.

Exercise 8.2.3. Is the Rubik's cube group 2-transitive on the set of edge facets?

The following result is one illustration of how unique the symmetric group and alternating group are. (Recall that the alternating group A_n was defined in example 82 above.)

Theorem 140. *If $k > 5$ and G is a group acting k-transitively on a finite set X then G is isomorphic to S_m or to A_n, for some $m \geq k$ or some $n \geq k+2$.*

Conversely, S_n acts n-transitively on $\{1, 2, ..., n\}$ and A_n acts $(n-2)$-transitively on $\{1, 2, ..., n\}$.

This is proven in [R].

Remark 14. We shall discuss an example of this in §§13.6, 13.7. We shall also, in conjunction with our group-theoretical determination of the Rubik's cube group proven later, be able to deduce from Theorem 140 the following

Corollary 141. *(a) The Rubik's cube group G acts* 6*-transitively on the corners, leaving the edges alone. It acts* 8*-transitively on the corners but may permute two edges.*

(b) The Rubik's cube group G acts 10*-transitively on the edges, leaving the corners alone. It acts* 12*-transitively on the edges but may permute two corners.*

8.3 Examples of isomorphisms

Example 142. Let G be the group in Exercise 8.1.2 and $f : G \to S_3$ the homomorphism. This is in fact an isomorphism.

Example 143. Let H be the subgroup of the Rubik's cube group generated by the basic move R: $H =< R >$. Then $H \cong C_4$ (where C_4 denotes the cyclic group of order 4).

Example 144. Recall that to each permutation g of the set $\{1, 2, ..., n\}$ we can associate a $n \times n$ permutation matrix $P(g)$ in such a way that

$$P(g) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{g(1)} \\ x_{g(2)} \\ \vdots \\ x_{g(n)} \end{pmatrix}.$$

Here the image of i under the permutation g is denoted $g(i)$, though in fact one plugs i into g from the left.) We let P_n denote the set of all $n \times n$ permutation matrices. This is a group under matrix multiplication. The function

$$\begin{aligned} P : S_n &\to P_n, \\ g &\longmapsto P(g) \end{aligned}$$

is an isomorphism. The proof that this is a bijection and a homomorphism was given earlier in the chapter on permutations.

Example 145. From [NST], we have the following table of isomorphisms:

name	notation	isomorphic to
symmetry group of tetrahedron	T	S_4
rotation group of tetrahedron	ST	A_4
symmetry group of octahedron	O	$S_4 \times C_2$
rotation group of octahedron	SO	S_4
symmetry group of icosahedron	I	$A_5 \times C_2$
rotation group of icosahedron	SI	A_5
symmetry group of regular n-gon		D_{2n}, n odd $D_n \times C_2$, n even
rotation group of regular n-gon		D_n

Example 146. This example may be found in [B].

Let Q denote the quaternion group:

$$Q = \{1, -1, i, -i, j, -j, k, -k\},$$

where $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, and in general, $xy = -yx$ for x, y belonging to i, j, k. Then Q is isomorphic to the group

$$Q^* =< a, b > < \ G,$$

where

$$a = F^2 * M_R * U^{-1} * M_R^{-1} * U^{-1} * M_R * U * M_R^{-1} * U * F^2,$$
$$b = F * U^2 * F^{-1} * U^{-1} * L^{-1} * B^{-1} * U^2 * B * U * L,$$

via the map $f : Q^* \to Q$ defined by $\phi(a) = i$, $\phi(b) = k$.

The proof of this claim will be formulated in a later chapter as an exercise. (The easiest way to prove this uses ideas we haven't yet introduced.)

Exercise 8.3.1. As above, let G be a group and h a fixed element of G. Define $c_h : G \to G$ by

$$c_h(g) = h * g * h^{-1}, \qquad g \in G.$$

Show that this is an automorphism.

Definition 147. An automorphism as in the above exercise is called inner. An automorphism of G which is *not* of this form, for some $h \in G$, is called outer.

(solution to Exercise 8.3.1: To verify this, we must show that $f = c_h$ is an injective and surjective homomorphism (we drop the subscript for simplicity of notation).

First, we show that f is injective. Suppose $f(g_1) = f(g_2)$. Then $f(g_1 * g_2^{-1}) = 1$, so that $h * g_1 * g_2^{-1} * h^{-1} = 1$. Multiply both sides of this equation on the left by h and on the right by h^{-1}. We obtain $g_1 * g_2^{-1} = 1$. This implies $g_1 = g_2$, so f is injective.

Now we show f is surjective. Let g be an arbitrary but fixed element of G. Let $y = h^{-1} * x * h$. Then

$$f(y) = f(h^{-1} * x * h) = h * h^{-1} * x * h * h^{-1} = x.$$

Therefore, f is surjective.

We verified previously that f is a homomorphism.)

Notation: The set of all automorphisms of a group G is denoted $Aut(G)$. The subset of inner automorphisms is denoted

$$Inn(G) := \{f \in Aut(G) \mid f = c_h, \text{ some } h \in G\},$$

in the notation of the above 8.3.1.

Exercise 8.3.2. (a) Show $Aut(G)$ is a group with composition as the group operation.

(b) Show that $Inn(G)$ is a subgroup of $Aut(G)$.

(c) Show that the function $\phi : G \to Inn(G)$ defined by $\phi(h) = c_h$ is a homomorphism.

8.3.1 Conjugation in S_n

The following result will be of importance to us in a later chapter:

Lemma 148. *Suppose $f : S_n \to S_n$ is an inner automorphism. If $g \in S_n$ is a disjoint product of cycles of length $k_1, ..., k_r$ then $f(g)$ is a disjoint product of cycles of length $k_1, ..., k_r$.*

In other words, an inner automorphism (i.e., conjugation) must "preserve the cycle structure". Lemma 50 , whose proof was promised earlier, follows from this.

proof: Since f is inner, let it be conjugation by $h \in S_n$ say, so $f(g) = h^{-1}gh$, for all $g \in S_n$. Let $(i)g \in \{1, ..., n\}$ denote the image of $i \in \{1, ..., n\}$

under $g \in S_n$. The lemma is a consequence of the following simple calculation: if $(i)g = j$ then, for all $1 \leq i \leq n$, we have

$$((i)h)(h^{-1}gh) = (j)h. \tag{8.1}$$

In other words, if g sends $i \longmapsto j$ then $h^{-1}gh$ sends $(i)h \longmapsto (j)h$. It follows that g and $h^{-1}gh$ have the cycle structure. $\square$

Theorem 149. *Two elements $g, g' \in S_n$ are conjugate if and only if they have the same cycle structure.*

proof: The Lemma proves the "only if" direction of this equivalence. Suppose that $g, g' \in S_n$ have the same cycle structure. Write their disjoint cycle decompositions using the lexicographical ordering imposed on the lengths of the cycles occurring in the decomposition: say

$$g = (i_1 \ ... \ i_{n_1})(i_{n_1+1} \ ... \ i_{n_2})...(i_{n_k+1} \ ... \ i_n),$$
$$g' = (i'_1 \ ... \ i'_{n_1})(i'_{n_1+1} \ ... \ i'_{n_2})...(i'_{n_k+1} \ ... \ i'_n),$$

where $1 \leq n_1 < ... < n_k < n$. Pick an $h \in S_n$ such that $h : i_j \longmapsto i'_j$, for all $1 \leq j \leq n$. Then $g' = h^{-1}gh$, by (8.1). $\square$

8.3.2 Aside: Automorphisms of S_n

Though we shall not need it here, the following fact is interesting since it illustrates what a unique role the symmetric group S_6 plays in the family of all symmetric groups.

Theorem 150. *If $n \neq 2, 6$ then the homomorphism $\phi : S_n \to Aut(S_n)$ (in part (c) of the exercises above) is an isomorphism:*

$$S_n \cong Aut(S_n).$$

If $n = 6$ then $|Aut(S_6)| = 2 \cdot |S_6|$.

Continuing our example from the appendix to the above chapter on the Platonic solids:

Example 151. Any permutation of the 6 diagonals of the icosahedron, which may be regarded as an element of S_6, gives rise to a permutation of the set

of 6 pentads, which may also be regarded as an element of S_6. This gives a map

$$f : S_6 \to S_6,$$

which is in fact a homomorphism. This homomorphism is injective so it is actually an automorphism.

However, a 2-cycle on the set of 6 diagonals (i.e., swapping exactly 2 diagonals) does *not* induce a 2-cycle on the set of these 6 pentads. In fact, a 2-cycle on the set of diagonals gives rise to a product of three disjoint 2-cycles on the set of these 6 pentads. Therefore, by the above theorem (which says that an inner automorphism must preserve the cycle structure) this automorphism f cannot be an inner automorphism.

8.4 Kernels and normal subgroups

Let $f : G_1 \to G_2$ be a homomorphism between two groups. Let

$$ker(f) = \{g \in G_1 \mid f(g) = e_2\},$$

where e_2 is the identity element of G_2. This set is called the kernel of f.

Lemma 152. *$ker(f)$ is a subgroup of G_1.*

Exercise 8.4.1. Prove this.

Example 153. Let

$$sgn : S_n \to \{\pm 1\}$$

denote the homomorphism which associates to a permutation either 1, if it is even, or -1, if it is odd. Then $A_n = ker(sgn) \subset S_n$.

The following properties of the kernel are useful:

Lemma 154. *: Let $f : G_1 \to G_2$ be a homomorphism between two groups.*

(a) f is injective if and only if $ker(f) = \{e_1\}$.

(b) if g belongs to the kernel and x is any element of G_1 then $x^{-1} * g * x$ must also belong to the kernel.

proof: (a) f is injective if and only if $f(g_1) = f(g_2)$ implies $g_1 = g_2$ $(g_1, g_2 \in G_1)$. Note $f(g_1) = f(g_2)$ is true if and only if $f(g_1 * g_2^{-1}) = e_2$. If $ker(f) = \{e_1\}$ then $f(g_1 * g_2^{-1}) = e_2$ implies $g_1 * g_2^{-1} = e_2$, which implies $g_1 = g_2$, which implies f is injective.

Therefore, if $ker(f) = \{e_2\}$ then f is injective. Conversely, if f is injective then $f(x) = f(e_1)(= e_2)$ implies $x = e_1(x \in G_1)$. This implies $ker(f) = \{e_1\}$.

(b) Multiply both sides of $e_2 = f(g)$ on the left by $f(x)^{-1}$ and on the right by $f(x)$. We get

$$e_2 = f(x)^{-1} * e_2 * f(x) = f(x^{-1}) * f(g) * f(x) = f(x^{-1} * g * x),$$

as desired. □

Definition 155. Let H be a subgroup of G. We say that H is a normal subgroup if, for each $g \in G$, $g^{-1} * H * g = H$ (i.e., for each $g \in G$ and each $h \in H, g^{-1} * h * g$ belongs to H).

Notation: Sometimes we denote "H is a normal subgroup of G" by

$$H \triangleleft G$$

Example 156. $A_n \triangleleft S_n$ and $|A_n| = \frac{1}{2}|S_n|$.

We have already shown the following

Lemma 157. *If $f : G_1 \to G_2$ is a homomorphism between two groups then $ker(f)$ is a normal subgroup of G_1.*

Remark 15. The following remarkable result about the alternating group will not be needed in this course, except as an example of a group with no normal subgroups provided for the readers' cultural benefit. It will not be proven here. (For a proof, see for example [R].) It is - believe it or not - connected with the fact that you cannot solve the general polynomial of degree 5 or higher using radicals, i.e., that there is no analog of the quadratic formula for polynomials of degree 5 or higher.

Theorem 158. *If X has 5 elements or greater then A_X has no non-trivial proper normal subgroups. In other words, if $H \triangleleft A_X$ is a normal subgroup then either $H = \{1\}$ or $H = A_X$.*

The next fact about the alternating group will be needed later in our determination of the structure of the Rubik's cube group. This fact also arose in connection with our previous discussion of the "legal positions" of the 15 puzzle.

Proposition 159. *Let H be the subgroup of S_n generated by all the 3-cycles in S_n then $H = A_n$.*

proof: Since $sgn : S_n \to \{\pm 1\}$ is a homomorphism, and since any 3-cycle is even, any product of 3-cycles must also be even. Therefore, $H \subset A_n$. If $g \in A_n$ then g must swap an even number of the inequalities $1 < 2 < ... < n-1 < n$, by Definition 37. Therefore, (since any permuation may be written as a product of 2-cycles, Theorem 58) g must be composed of permutations of the form $(i\ j)(k\ l)$ or $(i\ j)(j\ k)$. But $(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l)$ and $(i\ j)(j\ k) = (i\ j\ k)$. Therefore, $g \in H$. This implies $A_n \subset H$, so $A_n = H$. □

The following more precise result is very useful for the purposes of the analsis of permutation puzzles.

Lemma 160. *([W]) Let X be a finite set, $|X| \geq 3$ and fix u, v as elements in X. Then the 3-cycle (u, v, x), x an element of $X - \{u, v\}$, generates A_X. This lemma proves an even stronger statement than the previous claim. Now, instead of only one element being fixed, there are two elements fixed and the group is still generated.*

8.5 Quotient subgroups

One of the most useful facts about normal subgroups is the following:

Lemma 161. *If H is a normal subgroup of G then G/H is a group with the following operation:*

$$aH * bH = (ab)H, \qquad (aH)^{-1} = a^{-1}H,$$

for all a, b belonging to G. The identity element of this group is the trivial coset H.

Exercise 8.5.1. Prove this.

This group G/H is called the quotient group of G by H and is sometimes pronounced "G mod H".

Example 162. If $f : G_1 \to G_2$ is a homomorphism between two groups then $G_1/ker(f)$ is a group.

The "basic building blocks" of the collection of finite groups are the groups which have no non-trivial quotient groups. Intuitively, this is because a non-trivial quotient group is closely related to the original group but smaller in size (and hence perhaps subject to analysis by an inductive argument of some type). These "basic" groups are called "simple":

Definition 163. A simple group is a group with no proper normal subgroups other than the trivial subgroup $\{1\}$.

Example 164. If p is a prime then C_p (the cyclic group having p elements) is simple. In fact, if G is any group which is both abelian and simple then there is a prime p such that $G \cong C_p$. If $n > 4$ then A_n is simple (as was stated above in Theorem 158). These facts are proven in [R].

Simple groups are not very abundant. In fact, the first non-abelian simple group is of order 60 (it's A_5).

The following basic result describes the quotient group $G_1/ker(f)$.

Theorem 165. *("first isomorphism theorem") If $f : G_1 \to G_2$ is a homomorphism between two groups then $G_1/ker(f)$ is isomorphic to $f(G_1)$.*

proof: $ker(f)$ is a normal subgroup of G_1, so $G_1/ker(f)$ is a group. We must show that this group is isomorphic to the group $f(G_1)$. Define $\phi : G_1/ker(f) \to f(G_2)$ by $\phi(g \cdot ker(f)) = f(g)$, for $g \in G_1$. We must show

(a) ϕ is well-defined,

(b) ϕ is a homomorphism,

(c) ϕ is a bijection.

If $g \cdot ker(f) = g' \cdot ker(f)$ then $g^{-1}g' \in ker(f)$, since $ker(f)$ is a group. This implies $f(g^{-1}g') \in f(ker(f)) = \{1\}$, so $f(g) = f(g')$. This implies ϕ is well-defined.

Since $ker(f)$ is normal, $(g \cdot ker(f))(g' \cdot ker(f)) = gg'(g'^{-1}ker(f)g')ker(f) = gg' \cdot ker(f)$. Therefore $\phi((g \cdot ker(f))(g' \cdot ker(f))) = \phi(gg' \cdot ker(f)) = f(gg') = f(g)f(g') = \phi(g \cdot ker(f))\phi(g' \cdot ker(f))$, for all $g, g' \in G$. This implies ϕ is a homomorphism.

It is clear that ϕ is surjective. To show that ϕ is a bijection, it suffices to prove ϕ is an injection. Suppose that $\phi(g \cdot ker(f)) = \phi(g' \cdot ker(f))$, for some $g, g' \in G$. Then $f(g) = f(g')$, so $f(g^{-1}g') = 1$. By definition of the kernel, this implies $g^{-1}g' \in ker(f)$, so $g \cdot ker(f) = g' \cdot ker(f)$. This implies ϕ is injective.

□

The other isomomorphism theorems will not be needed but will be stated to help to illustrate the usefulness of the notion of normality:

Theorem 166. *("second isomorphism theorem") If H, N are subgroups of a group G and if N is normal then*

(a) $H \cap N$ is normal in H,

(b) there is an isomorphism

$$H/(H \cap N) \cong NH/N.$$

Theorem 167. *("third isomorphism theorem") If N_1, N_2 are subgroups of a group G, if $N_1 \subset N_2$, and if N_1 and N_2 are both normal then*
(a) N_2/N_1 is normal in G/N_1,
(b) there is an isomorphism between

$$(G/N_1)/(N_2/N_1) \cong G/N2.$$

We shall not prove these results here - see [G] or [R].

8.6 Direct products

Definition 168. Let H_1, H_2 be two subgroups. We say that a group G is the direct product of H_1 with H_2, written

$$G = H_1 \times H_2,$$

if
(a) $G = H_1 \times H_2$ (Cartesian product, as sets),
(b) the group operation on G is given "coordinate-wise" (still denoted "$*$" for simplicity):

$$(x_1, y_1) * (x_2, y_2) = (x_1 * x_2, y_1 * y_2),$$

for $x_1, x_2 \in H_1,\ y_1, y_2 \in H_2$ (where $*$ denotes multiplication in H_1, H_2, and G).

Example 169. Let G be (as a set) the Cartesian product $G = C_2^2$, where $X^2 = X \times X$ and where C_2 denotes the cyclic group of order 2 (with addition mod 2 as the operation). Define addition on G coordinate-wise:

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2),$$

where $0 \leq m_i \leq 1$, $0 \leq n_j \leq 2$, for $i = 1, 2,\ j = 1, 2$.

Example 170. The symmetry group O of the octahedron is isomorphic to $S_4 \times C_2$. The symmetry group I of the icosahedron is isomorphic to $A_5 \times C_2$. (This is not isomorphic to S_5, despite the fact that they both have the same number of elements and they both contain A_5 as a normal subgroup.)

8.7 Examples

Example 171. Consider the subgroup H of the Rubik's cube group generated by the "square slice moves",

$$H =< M_R^2, M_D^2, M_U^2 > .$$

Then $H =< M_R^2 > \times < M_D^2 > \times < M_U^2 > \cong C_2 \times C_2 \times C_2 = C_2^3$.

8.7.1 The twists and flips of the Rubik's cube

We recall some notation:

- X is the set of 48 facets of the Rubik's cube which are not center facets,
- V denotes the subset of facets which belong to some corner subcube,
- E is the subset of facets which belong to some edge subcube.
- Let G denote the Rubik's cube group.
- Let F be the group generated by all the moves of the Rubik's cube group which do not permute any corner or edge subcubes but may twist or flip them.
- Let S_X, S_V, S_E, denote the symmetric group on X, V, E, respectively. We may regard F, G, as subgroups of S_X. We may also regard S_V, S_E as subgroups of S_X (for example, S_V is the subgroup of S_X which leaves all the elements of E fixed).
- Let

$$G_V = S_V \cap G, \quad G_E = S_E \cap G, \quad F_V = S_V \cap F, \quad F_E = S_E \cap F.$$

Note that the action of G on X induces an equivalence relation as follows: we say that a facet f_1 is equivalent to a facet f_2 if there is a move of the Rubik's cube which sends one facet to the other. There are exactly two equivalence classes, or orbits, of G in X: namely, V and E. In particular, the action of G on V is transitive and the action of G on E is transitive. On the other hand, F leaves each vertex (resp., edge) fixed, though it may permute the corner facets (resp., edge facets) associated to a vertex (resp., edge).

Exercise 8.7.1. Show that:

(a) The set $\overline{V}$ of equivalence classes of F acting on V is in bijective correspondence with the set of all vertices of the cube.

(b) The set $\overline{E}$ of equivalence classes of F acting on E is in bijective correspondence with the set of all edges of the cube.

The interesting thing is that we have

$$F = F_V \times F_E \qquad \text{(direct product)}.$$

Exercise 8.7.2. Notation as above.

(a) Show $F = F_V \times F_E$ (direct product).

(b) Is $S_X = S_V \times S_E$ (direct product)?

A harder question, which we will answer later in the negative: Is $G = G_V \times G_E$ (direct product)?

8.7.2 The slice group of the Rubik's cube

The material below can also be found in [BH]. Some ideas are also discussed in [Si].

Let H be the group $< M_R, M_F, M_U >$ generated by the middle slice moves. This group is called the "slice group". Let E be the set of edges of the cube (which we identify with the set of edge subcubes), let C be the set of center facets of the cube, and let $X = E \cup C$. H acts on X. Note that H does not affect the corners (i.e, the vertices of the cube).

Questions: (a) Is the action of H on X transitive?

(b) Is the action of H on C transitive?

(c) Is the action of H on E transitive?

The answer to (a) is no - an edge subcube cannot be sent to a center facet, for example, so there is an element of X which cannot be sent to any other element of X by an element of H. The answer to (b) is yes - any center facet can be sent to any other center facet by an element of H. The answer to (c) is no - for example, the uf edge subcube cannot be sent to the ur edge subcube by a slice move, so there is an element of E which cannot be sent to any other element of E by an element of H.

The answer of "no" to (c) brings about the following

Question: What are the orbits of H on E?

The answer may be phrased in various ways, but let us look at it in the following way: suppose we call two edge subcubes equivalent if one can be

sent to the other by a slice move (i.e., an element of H). There are 3 disjoint equivalence classes: all the subcubes in the middle RL-slice are equivalent, all the subcubes in the middle FB-slice are equivalent, and all the subcubes in the middle UD-slice are equivalent. The distinct orbits of H acting on E are the following:

- the middle RL-slice, denoted by E_{RL},
- the middle FB-slice, denoted by E_{FB},
- the middle UD-slice, denoted by E_{UD}.

Note that

$$E = E_{RL} \cup E_{FB} \cup E_{UD},$$

is a partitioning of E into the distinct equivalence classes defined by the action of H on E.

Each element of H determines an element in S_X. We have a homomorphism

$$f : H \to S_X$$

This is another way of saying that H acts on the set X, which we already know. Note that each basic slice move M (so M is either M_R, M_F, or M_U) is, as an element of S_X, of the following form:

$$M = (4 - \text{cycle in } S_E)(4 - \text{cycle in } S_C).$$

Conversely, does an element of S_X uniquely determine an element of H? In other words, is f injective (i.e., an embedding)?

To answer this, fix an $h \in H$ and think about what $f(h)$ tells us: $f(h)$ tells us which each subcube moves to which other subcube but it doesn't tell us, for example, how a subcube is flipped or rotated.

The fundamental theorem 60 inspires the following question:

Question: Can an element of H flip, but not permute, an edge subcube (and possibly permuting or flipping other subcubes of the cube)?

The answer is no. The reason why is that the slice moves can only rotate a given edge subcube within the slice it belongs to.

It follows, therefore, that the permutations of the edge subcube and centers determine a unique element of the slice group. In other words, we have proven the following

Proposition 172. *The homomorphism*

$$f : H \to S_X$$

is an embedding.

Remark 16. The analog of this for the Rubik's cube group is false!

H acts on the set E_{RL}, so we have a homomorphism

$$r_{RL} : H \to S_{E_{RL}}$$

and similarly, $r_{UD} : H \to S_{E_{UD}}$, $r_{FB} : H \to S_{E_{FB}}$.

H acts on each of the sets E and C, so we have homomorphisms

$$r = r_{RL} \times r_{UD} \times r_{FB} : H \to S_{E_{RL}} \times S_{E_{UD}} \times S_{E_{FB}} \subset S_E, \qquad s : H \to S_C,$$

which we can put together to obtain an injective homomorphism

$$r \times s : H \to S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C$$

To determine H, we determine the image of H in $S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C$.

To do this, we first look at the image of H in each of $S_{E_{RL}}$, $S_{E_{FB}}$, and $S_{E_{UD}}$. This is easy enough:

- the image of H in $S_{E_{RL}}$ is $< M_R > \cong C_4$,
- the image of H in $S_{E_{FB}}$ is $< M_F > \cong C_4$,
- the image of H in $S_{E_{UD}}$ is $< M_U > \cong C_4$.

Later, we shall want to think of C_4 as $\{0, 1, 2, 3\}$, with addition mod 4, and the image of an element $h \in H$ under one of the homomorphisms above, $r_{RL} : H \to S_{E_{FB}}$ say, as an integer $0 \leq r_{RL}(h) \leq 3$.

Next, we must determine the image of H in S_C. This is easy if it's looked at in the right way. As far as the movements of the center facets is concerned, the slice moves may be replaced by their corresponding rotations of the entire cube about an axis of symmetry. In this case, we see that the image of H in S_C is the same as the image of the orientation-preserving symmetry group of the cube! This we know, by the discussion in chapter 7 and Example 145 above, is isomorphic to S_4.

Putting all this together, we see that the image of H in $S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C$ is isomorphic to a subgroup of

$$C_4^3 \times S_4.$$

We may represent the elements of H , therefore, as 4-tuples (h_1, h_2, h_3, h_4), with $h_1, h_2, h_3 \in C_4$ and $h_4 \in S_4$. Since each of the generating moves of H (namely, M_R, M_U, and M_F) satisfies

$$sgn(r(h)) = sgn(s(h)),$$

for all $h \in H$, the image of H cannot be all of $C_4^3 \times S_4$.

Proposition 173. *The image of H in $C_4^3 \times S_4$. is isomorphic to the kernel of the map*

$$\begin{gathered} t : C_4^3 \times S_4 \to \{\pm 1\} \\ (h_1, h_2, h_3, h_4) \longmapsto sgn(h_1) \cdot sgn(h_2) \cdot sgn(h_3) \cdot sgn(h_4), \end{gathered}$$

where each sgn is the sign of the permutation, regarded as an element of S_X.

Exercise 8.7.3. Show that $|ker(t)| = (4^3 \cdot 4!)/2 = 768$.

proof: We have shown that H is isomorphic to a subgroup of $C_4^3 \times S_4$. In fact, we know that the basic slice moves M_R, M_U, M_F (which generate H) all belong to the kernel of t, so H is isomorphic to a subgroup of $ker(t) < C_4^3 \times S_4$.

It remains to show that every element in $ker(t)$ belongs to H. To do this, we consider the projection homomorphism

$$p : H \to S_4$$

obtained by composing the homomorphism $r \times s : H \to C_4^3 \times S_4$ constructed above with the projection homomorphism $C_4^3 \times S_4 \to S_4$. We have shown that p is surjective. Our next objective is to compute the kernel of p and use the first isomorphism theorem to determine H.

Claim: The kernel of p is

$$ker(p) = \{h \in H \mid s(h) = 1,\ r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}.$$

Note that $ker(p)$ is a subgroup of H so the sign of the permutation $s(h)$ is equal to the sign of the permutation $r(h)$:

$$sgn(s(h)) = sgn(r(h)) = sgn(r_{RL}(h)) \cdot sgn(r_{UD}(h)) \cdot sgn(r_{FB}(h)).$$

This implies that

$$ker(p) \subset \{h \in H \mid s(h) = 1,\ r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}.$$

Conversely, pick an $h \in H$ such that $s(h) = 1$ and $r_{RL}(h)+r_{UD}(h)+r_{FB}(h) \equiv 0 \pmod 2$. We may represent this element h as a 4-tuple (n_1, n_2, n_3, s), with $0 \leq n_1, n_2, n_3 \leq 3$ and $s = 1 \in S_4$.

For example,

- the element $M_1 = M_R * M_F^{-1} * M_D * M_F$ is represented by the 4-tuple $(1, 1, 0, 1)$,
- the element $M_2 = M_R * M_D * M_F * M_D^{-1}$ is represented by the 4-tuple $(0, 1, 1, 1)$,
- the element $M_3 = M_F * M_D * M_R^{-1} * M_D^{-1} * M_F * M_D^{-1} * M_R * M_D$ is represented by the 4-tuple $(0, 0, 2, 1)$.

These elements generate all the elements of the group

$$\{(a, b, c, 1) \mid a, b, c \in C_4,\ a + b + c \equiv 0 \pmod 2\}.$$

Note that the group $\{(a, b, c) \mid a, b, c \in C_4,\ a+b+c \equiv 0 \pmod 2\}$ is, in turn, the kernel of the map $C_4^3 \to C_2$ given by $(a, b, c) \longmapsto a + b + c \equiv 0 \pmod 2$.

Exercise 8.7.4. Show that $|\{(a, b, c) \mid a, b, c \in C_4,\ a + b + c \equiv 0 \pmod 2\}| = 4^3/2 = 32$.

Therefore, the element h choosen above must be expressible as a "word" in these three elements M_1, M_2, M_3. This shows that

$$\{h \in H \mid s(h) = 1,\ r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\} \subset ker(p),$$

which implies the claim.

To summarize what we have so far: we have a surjective homomorphism $p : H \to S_4$ with kernel $\{h \in H \mid s(h) = 1,\ r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}$. The kernel has $|ker(p)| = 32$ elements and the image has $|im(p)| = |S_4| = 4! = 24$ elements. Since, by the first isomomorphism theorem,

$$H/ker(p) \cong S_4,$$

we have $|H| = 32 \cdot 24 = 768$. But the kernel of the homomorphism $t : C_4^3 \times S_4 \to \{\pm 1\}$, which we know contains H as a subgroup, also has 768 elements. This forces $h = ker(t)$. $\square$

The slice group of the megaminx

The subgroup S of the megaminx group generated by all elements of the form $x * y^{-1}$, where x, y correspond to faces which have *no intesection* is called the slice group of the megaminx.

Problem (Longridge): Determine S.

8.8 Semi-direct products

If a group G contains two subgroups H_1 and H_2, with $H_1 \lhd G$ normal, such that each element of G can be written uniquely as a product $h_1 h_2$, with $h_1 \in H_1$ and $h_2 \in H_2$ then we say that G is the semi-direct product of H_1 and H_2. In this situation, H_2 is called a complement of H_1. In this section, we shall define two more ways of seeing how a semi-direct product can be expressed. Later, we shall see that the Rubik's cube group is an easily described subgroup of a certain semi-direct product.

Definition 174. Now suppose that H_1, H_2 are both subgroups of a group G.

We say that G is the semi-direct product of H_1 by H_2, written

$$G = H_1 \ {>\!\lhd} \ H_2$$

if

(a) $G = H_1 * H_2$,

(b) H_1 and H_2 only have 1, the identity of G, in common,

(c) H_1 is normal in G.

This is the "internal version" of the semi-direct product.

Of course, if we define anything using two apparently different definitions, we'd better be sure that they are equivalent! The fact that they are is a theorem (Theorem 7.23 in [R]) which we won't prove here.

Note that the multiplication rule in G doesn't have to be mentioned since we are assuming here that G is given.

The "external version" is defined by a construction as follows:

Definition 175. Assume we have a homomorphism

$$\phi : H_2 \to Aut(H_1).$$

Define multiplication on the set $H_1 \times H_2$ by

$$(x_1, y_1) * (x_2, y_2) = (x_1 * \phi(y_1)(x_2), y_1 * y_2).$$

This defines a group operation. This group, denoted $H_1 >\!\lhd_\phi H_2$, is the (external) semi-direct product.

This definition will be used with the example of $H_1 = C_m^n$ and $H_2 = S_n$ in the next chapter.

These last two definitions are equivalent by Theorems 7.22-7.23 in [R].

As a set, $H_1 >\!\lhd H_2$ is simply the Cartesian product $H_1 \times H_2$.

Example 176. Let $\mathbb{R}^2$ denote the direct product of the additive group of real numbers with itself:

$$\mathbb{R}^2 = \{(x, y) \mid x, y \text{ real}\},$$

with the group operation being addition performed componentwise. Let C_2 denote the multiplicative cyclic group with 2 elements, whose elements we write (somwhat abstractly) as $C_2 = \{1, s\}$. (We may think of s as being equal to -1 but there is a reason for this notation which shall be made clear soon.) Define an action of C_2 on $\mathbb{R}^2$ by

$$1(x, y) = (x, y), \qquad s(x, y) = (y, x), \qquad (x, y) \in \mathbb{R}^2.$$

Let G be the set

$$G = \mathbb{R}^2 \times C_2.$$

Define the binary operation $* : G \times G \to G$ by

$$(g_1, z_1) * (g_2, z_2) = (g_1 + z_1(g_2), z_1 * z_2),$$

for all $g_1, g_2 \in G$ and all $z_1, z_2 \in C_2$. This is a group - the semi-direct product of $\mathbb{R}^2$ with C_2.

To see this, we must answer some questions:

(a) closed under the operation? Yes

(b) existence if identity? Yes, $e = ((0, 0), 1)$

(c) existence of inverse? Yes, $((x, y), 1)^{-1} = ((-x, -y), 1)$, and $((x, y), s)^{-1} = ((-y, -x), s)$.

(d) associative? This is the hard one:

$$\begin{aligned}((g_1, z_1) * (g_2, z_2)) * (g_3, z_3) &= (g_1 + z_1(g_2), z_1 * z_2) * (g_3, z_3) \\ &= (g_1 + z_1(g_2) + (z_1 * z_2)(g_3), (z_1 * z_2) * z_3) \\ (g_1, z_1) * ((g_2, z_2) * (g_3, z_3)) &= (g_1, z_1) * (g_2 + z_2(g_3), z_2 * z_3) \\ &= (g_1 + z_1(g_2) + z_1(z_2(g_3)), z_1 * (z_2 * z_3))\end{aligned}$$

This implies associativity.

Exercise 8.8.1. Let G be the semi-direct product constructed in the above example. Show that $\mathbb{R}^2$ (which we identify with the subgroup $\{((x,y),1) \mid (x,y) \in \mathbb{R}^2\}$ of G) is a normal subgroup.

Example 177. Let

$$S_3 = \{1, s_1, s_2, s_1 * s_2, s_2 * s_1, s_1 * s_2 * s_1\}, \;\; H_1 = \{1, s_2, s_1 * s_2 * s_1\}, \;\; H_2 = \{1, s_1\}.$$

Let

$$\phi : H_2 \to Aut(H_1)$$

be defined by

$$\begin{array}{c} \phi(1) = 1 \;\; \text{(the identity automorphism)} \\ \phi(s_1)(h) = s_1^{-1} * h * s_1 = s_1 * h * s_1 \end{array}$$

(since $s_1^{-1} = s_1$), $h \in H_1$.

Define the (external) semi-direct product of H_1, H_2 by $G = H_1 >\!\lhd H_2$.

Exercise 8.8.2. Let G be the semi-direct product constructed in the above example. Show that H_1 (which we identify with the subgroup $\{(h,1) \mid h \in H_1\}$ of G) is a normal subgroup.

There is of course a close relationship between internally defined semi-direct products and externally defined ones. The following lemma, which is proven in [R], explains this connection:

Lemma 178. *If G is the (internal) semi-direct product of H_1 by H_2 (so H_1 is a normal subgroup of G) then there is a homomorphism*

$$\phi : H_2 \to Aut(H_1)$$

such that $G \cong H_1 >\!\lhd_\phi (H_2)$.

Example 179. Let C_d be the cyclic group of order d, which we may regard as a set as $C_r = \{0, 1, ..., d\}$, with addition performed mod d. Let $N = C_d^n$, which we regard as the group of "n-vectors" with "coefficients" in C_d. Let $H = S_n$ be the symmetric group on n letters, i.e., the group of all permutations

$$p : \{1, 2, ..., n\} \to \{1, 2, ..., n\}.$$

The group H acts on N by permuting the indices, i.e., the coordinates of the vectors. For $p \in S_n$, define $p^* : C_d^n \to C_d^n$ by

$$p^*(v) = (v_{p^{-1}(1)}, ..., v_{p^{-1}(n)}), \qquad v = (v_1, ..., v_n) \in C_d^n.$$

Now, for $p, q \in S_n$ and $v, w \in C_d^n$, define

$$(p, v) * (q, w) = (pq, w + q(v)).$$

This defines a semi-direct product $C_d^n >\lhd S_n$.

(It is known that $C_d^n >\lhd S_n$ is isomorphic to the group of all "C_n-valued $n \times n$ monomial matrices", [R], Exercise 7.33. A monomial matrix is a matrix which contains exactly one non-zero entry for each row and column.)

8.9 Wreath products

Let G_1 be a group, let G_2 be a group acting on a finite set X_2. Fix some labeling of X_2 as say $X_2 = \{h1, h2, ..., h_m\}$, where $m = |X_2|$ and let $G_1^{X_2}$ denote the direct product of G_1 with itself m times, with the coordinates labeled by the elements of X_2.

Definition 180. The wreath product of G_1, G_2 is the group

$$G_1 \operatorname{wr} G_2 = G_1^{X_2} >\lhd G_2$$

where the action of G_2 on $G_1^{X_2}$ is via its action on X_2.

In particular, to each $t \in G_1 \operatorname{wr} G_2$ there is a $g_2 \in G_2$. We denote this projection by $g_2 = pr(t)$. Define the base of the wreath product by

$$B = \{t \in G_1 \operatorname{wr} G_2 \mid pr(t) = 1\},$$

so $B = G_1^{X_2}$.

Example 181. Let $\mathbb{R}^n$ denote the direct product of the additive group of reals with itself n times. The group operation on $\mathbb{R}^n$ is componentwise addition. Let S_n denote the symmetric group. This acts on $\mathbb{R}^n$ by permuting coordinates: if $r \in S_n$ is a permutation then define

$$r(x_1, ..., x_n) = (x_{r(1)}, ..., x_{r(n)}),$$

for $(x_1..., x_n) \in \mathbb{R}^n$. This action respects the addition operation:

$$r(x_1 + y_1, ..., x_n + y_n) = r(x_1, ..., x_n) + r(y_1, ..., y_n),$$

$(x_1..., x_n), (y_1..., y_n) \in \mathbb{R}^n$. (Incidently, it also preserves scalar multiplication:

$$r(a * (x_1, ..., x_n)) = a * r(x_1, ..., x_n),$$

for $(x_1..., x_n) \in \mathbb{R}^n, a \in \mathbb{R}$, so r defines an invertible linear transformation on $\mathbb{R}^n$; in fact, there is a homomorphism $S_n \to Aut(\mathbb{R}^n)$, where $Aut(\mathbb{R}^n)$ denotes the group of all invertible linear transformations on $\mathbb{R}^n$; do you recognize this homomorphism? It has occurred previously in the notes...)

Let G be the set

$$G = \mathbb{R}^n \times S_n$$

and define a binary operation $* : G \times G \to G$ by

$$(g_1, p_1) * (g_2, p_2) = (g_1 + p_1(g_2), p_1 * p_2),$$

for all $g_1, g_2 \in G$ and all $p_1, p_2 \in S_n$. This is a group.

(a) closed under the operation?

(b) existence if identity? $e = ((0, 0), 1)$

(c) existence of inverse? $((x, y), 1)^{-1} = ((-x, -y), 1)$, $((x, y), p)^{-1} = (-p^{-1}(x, y), p^{-1})$.

(d) associative? This is the hard one:

$$\begin{aligned}((g_1, p_1) * (g_2, p_2)) * (g_3, p_3) &= (g_1 + p_1(g_2), p_1 * p_2) * (g_3, p_3) \\ &= (g_1 + p_1(g_2) + (p_1 * p_2)(g_3), (p_1 * p_2) * p_3) \\ (g_1, p_1) * ((g_2, p_2) * (g_3, p_3)) &= (g_1, p_1) * (g_2 + p_2(g_3), p_2 * p_3) \\ &= (g_1 + p_1(g_2) + p_1(p_2(g_3)), p_1 * (p_2 * p_3))\end{aligned}$$

This implies associativity.

This group is the wreath product of $\mathbb{R}$ with S_n:

$$G = \mathbb{R} \operatorname{wr} S_n,$$

where $\mathbb{R}$ is the base.

Lemma 182. *(a) The base B, which is isomorphic to the direct product $G_1^{|X_2|}$, is a normal subgroup of $G_1 \operatorname{wr} G_2$,*

(b) $(G_1 \operatorname{wr} G_2)/B$ is isomorphic to G_2.

For this, we refer to chapter 8 of [NST] or to [R].

Example 183. Let H be the enlarged Rubik's cube group of all legal and illegal moves of the 3×3 Rubik's cube. In other words, in addition to the usual basic moves (namely, R, L, U, D, F, B), we allow you to take apart the cube and reassemble the corner and edge subcubes (but we do not allow you to remove stickers from the facets). Let C_3 denote the group of all rotations of a particular corner subcube by a 120 degree angle (actually, this group depends on the corner being rotated but since these groups are all isomorphic we drop the dependence from the notation). Let C_2 denote the group of all flips of a particular edge subcube (rotations by a 180 degree angle). (Again, this group depends on the edge being flipped but since these groups are all isomorophic we drop the dependence from the notation). Then we shall prove later that

$$H = (C_3 \operatorname{wr} S_V) \times (C_2 \operatorname{wr} S_E),$$

where V is the set of corner subcubes and E is the set of edge subcubes.

8.9.1 Application to order of elements in $C_m \operatorname{wr} S_n$

In some cases, wreath products turn out to be relatively concrete and familiar groups. Let $S(n, m)$ denote the group of all $n \times n$ monomial matrices with entries in C_m.

We begin with the following result:

Theorem 184. *There is an isomorphism between $C_m \operatorname{wr} S_n$ and the group $S(n, m)$ which sends an element $(\vec{v}, f) \in C_m \operatorname{wr} S_n$, $\vec{v} = (v_1, v_2, ..., v_n) \in C_m^n$ and $f \in S_n$, to the matrix $P(f)\vec{v}$.*

This follows from a result (see Theorem 197) which will be proven in the next chapter. It is also a special case of an exercise in [R]. In any case, it is clear from this that an element $(\vec{v}, f) \in C_m \operatorname{wr} S_n$, $\vec{v} = (v_1, v_2, ..., v_n) \in C_m^n$ and $f \in S_n$, is order d only if the permutation matrix $P(f)$ is order d. Indeed,

$$\begin{gathered}(\vec{v}, f)^2 = (\vec{v} + f(\vec{v}), f^2), \\ (\vec{v}, f)^3 = (\vec{v} + f(\vec{v}) + f^2(\vec{v}), f^3), \\ \vdots \\ (\vec{v}, f)^k = (\vec{v} + ... + f^{k-1}(\vec{v}), f^k).\end{gathered}$$

We conclude with the following classification of the elements of order d in the wreath product.

Lemma 185. *An element* $(\vec{v}, f) \in C_m \operatorname{wr} S_n$, $\vec{v} = (v_1, v_2, ..., v_n) \in C_m^n$ *and* $f \in S_n$, *is order* d *if and only if* $f^d = 1$ *and* $\vec{v} + ... + f^{d-1}(\vec{v}) = 0$.

This result can, in principle, be used in conjunction with with the explicit determination of the Rubik's cube group given later to determine all the elements of a given order. As an application, the elements of order 2 of the Rubik's cube group will be given later.

Chapter 9

The Rubik's cube and the word problem

Further details in the following background material may be found in [R], [MKS].

Definition 186. Given a list L of questions, a decision algorithm for L is a uniform set of unambiguous instructions which, when applied to any question in L gives the correct answer "yes" or "no" after a finite number of steps.

9.1 Background on free groups

Let $X = \{x_1, ..., x_n\}$ denote a set and X^{-1} a set disjoint from X whose elements we denote by $\{x_1^{-1}, ..., x_n^{-1}\}$. Assume that the map $x \longmapsto x^{-1}$ defines a bijection $X \to X^{-1}$. It will be convenient to let $x^1 = x, x_i^0 = 1$, where 1 is an element not belonging to $X \cup X^{-1}$ which we will call the identity element. A word on X is a sequence

$$w = (a_1, a_2, ..., a_N),$$

where $N > 0$ is some integer and each ai belongs to

$$X \cup X^{-1} \cup \{1\}.$$

The sequence of all 1's is called the empty word. The inverse of the word w is the word

$$w^{-1} = (a_N^{-1}, ..., a_1^{-1}).$$

If $a_i = y_i^{e_i}$, where e_i is in $\{0, 1, -1\}$ and $y_i \in X$, then we shall write the word w as $w = y_1^{e_1}...y_N^{e_N}$.

Example 187. Let $X = \{R, L, U, D, F, B\}$. The set of words on X are in a bijective correspondence with the set of sequences of basic moves you can make on the Rubik's cube.

We call a word $w = y_1^{e_1}...y_N^{e_N}$ on X reduced if either w is empty or if the exponents e_i are non-zero and if there are no $x \in X$ with x, x^{-1} adjacent in w.

Definition 188. The free group $F_n = F_X$ on the generators $x_1, ..., x_n$ is the group of all reduced words on X.

The proof that F_n is a group is not entirely easy (verifying the associativity property is perhaps the hardest part), see Theorem 11.1 in [R].

9.1.1 Length

If, in the notation above, $w = y_1^{e_1}...y_N^{e_N}$ is a reduced word (so $e_i \in \{0, 1, -1\}$) then we call N the length (or reduced length, to be more precise) of w.

If $G =< g_1, ..., g_k >\subset S_n$ is a finite permutation group generated by permutations g_1, ..., g_k then we may still define the notion of length:

Definition 189. Suppose $g \in G$ is not the identity, where G is a permutation group as above. Then g may be written

$$g = y_1^{e_1}...y_N^{e_N},$$

where each $y_i \in \{g_1, ..., g_k\}$ and where $e_i \in \{0, 1, -1\}$. The number N and the sets $\{y_1, ..., y_N\}$, $\{e_1, ..., e_N\}$ may not be unique for a given g but among all such possibilities there is at least one such that the value of N is minimum. We call this the length of g, denoted $\ell(g)$.

Let

$$P_G(t) = \sum_{g \in G} t^{\ell(g)}.$$

This is called the Poincaré polynomial of G.

The length of g is the distance in the Cayley graph between the vertex g and the vertex 1. As was mentioned in the chapter on graph theory, the problem of determining the largest possible distance in the Cayley graph of the Rubik's cube group is known as "God's algorithm" and is currently unsolved.

Example 190. Let $G = S_n$ with generators $g_i = (i, i+1)$, $i = 1, ..., n-1$. The Poincaré polynomial is known:

$$\Pi_{k=1}^{n} \frac{t^{k+1} - 1}{t - 1},$$

by [Hum], §3.15.

In case $n = 2$, this is

$$t^3 + 2t^2 + 2t + 1 = (t + 1)(t^2 + t + 1)$$

Problem What is the longest possible length of an element of the Rubik's cube group (with respect to the generators R, L, U, D, F, B)?

Problem What is the Poincare polyomial of the Rubik's cube group (with respect to R, L, U, D, F, B)?

9.1.2 Trees

We may represent the free group graphically as follows. We define the Cayley graph of F_n inductively:

- draw a vertex for each element of $X \cup X^{-1}$ (these are the vertices, V_1 say, for the words of length 1),
- Suppose we are given that you have already drawn all the vertices for the words of length $k-1$, V_{k-1} let's call them. For each $x \in X \cup X^{-1}$ and each $v \in V_{k-1}$, draw a vertex for each word of length k obtained by multiplying v by x on the right, $v * x$, and connect v and $v * x$ by an edge.

There are infinitely many vertices, each of which has degree $|X \cup X^{-1}|$. Moreover, this graph has no circuits or loops (i.e., no path of edges crosses back over onto itself). Such a graph is called a tree.

Example 191. Let $X = \{R, L, U, D, F, B\}$. The elements of the free group F_X correspond to the mechanically different sequences of basic moves you can make on the Rubik's cube. Of course, different sequences of moves may yield the same position of the Rubik's cube (e.g., R^4 and 1 are the same position but sequence of moves used to attain them are distinct).

There are infinitely many vertices of the Cayley graph of F_X, each of which corresponds to a mechanically distinct move of the Rubik's cube.

9.2 The word problem

There is a way to list all the elements of F_n, called the lexicographic ordering. We shall describe a way to list all the words in F_n as though they were in a dictionary. We shall give an algorithm for determining if a word $w \in F_n$ occurs before a word w', in which case we write $w < w'$. In the dictionary below, we shall, for example, distingish between the the identity 1 and the "non-reduced" word $x_1 * x_1^{-1}$.

The first element in this lexicographically ordered list is the word 1, the next $2n$ words are the words

$$x_1 < x_1^{-1} < ... < x_n < x_n^{-1}.$$

In general, we define $y_1..y_M < z_1...z_N$ if either (a) $M < N$ or (b) $M = N$ and $y_1 < z_1$ or $y_1 = z_1$ and $y_2 < z_2$ or $y_1 = z_1$ and $y_2 = z_2$ and $y_3 < z_3$ or ... .

List all the elements of F_n as

$$F_n = \{w_1, w_2, ...\},$$

so $w_1 = 1, w_2 = x_1, ...$ Let G be a subgroup of F_n or a permutation group $G =< g_1, ..., g_n >$. If G is a permutation group then we regard a word w_k as an element of G by substituting g_i for each $x_i, 1 \leq i \leq n$.

Definition 192. Fix a $g \in G$. We say that G has a solvable word problem if there is a decision algorithm for the list L of questions of the form: Is $w_k = g$ in G?

Claim: F_n has a solvable word problem.
proof The following decision algorithm yields a solvable word problem.

1. If w is a word not equal to 1 then underline the first occurance, if any, of the expression $x_i * x_i^{-1}$. If no such expression occurs in w then go to step 3, otherwise go to step 2.

2. delete the expression $x_i * x_i^{-1}$ from w and go to step 1.

3. If $w = 1$ then stop and return "yes", otherwise, stop and return "no". □

Claim: Each finite permutation group has a solvable word problem.

Exercise 9.2.1. Why?

Theorem 193. *A decision algorithm for the word problem for the Rubik's cube group with generators R, L, U, D, F, B is the same as an algorithm for solving the Rubik's cube.*

9.3 Generators, relations, and Plutonian robots

Here's a hypothetical situation: You and a friend each have a robot on the planet Pluto with a scrambled Rubik's cube. You and your friend also have duplicate cubes, scrambled the same way as your robots. (We will call the robots R^2D^2 and R^2B^2 if you don't mind!) These robots have manual dexterity but no preprogramming on how to solve the cube. Furthermore, assume it is very expensive to program different moves, so you want to teach the robot the smallest number of separate moves that you can. On the other hand, the moves need not be basic moves (U, R, ..) since it we will assume it costs roughly the same to teach the robot the move R as the move $R * U^2 * R^{-1}$, for example. Your solution will be a "word" in these taught moves. Again, to minimize the cost of transmission, you want the "word" to be absolutely as short as possible. A prize of 1 million dollars has been set up to the first of you who can get their robot to solve its cube.

In other words, we want to solve the word problem for the cube *and* we want to do it as efficiently as possible. Suppose we know we need n generators and we know that this is the smallest number. How do we make a "word" as short as possible? To make a word in these generators as small as possible, we must know all the "relations" between these generators so we can, if necessary, substitute them into the word and perform some cancelation. This is what this section is about.

Let X be a finite set, say $n = |X|$. Let Y be a set of reduced words on X. Let R be the smallest normal subgroup of F_n containing Y. Since R is normal, the quotient F_n/R is a group.

Definition 194. Let G be a group. We say that G has generators X and relations Y if G is isomorphic to F_n/R. A collection of generators and relations defining a group is called a presentation of the group.

As a matter of notation, an element $r \in R$ is written as an equation $r = 1$ in G.

Remark 17. For those with a background in topology: Serre [Ser], §3.3, gives a topological interpretation of R as "the fundamental group of the Cayley graph of G with respect to X".

Example 195. The cyclic group of order 3, C_3, has one generator x and one relation $x^3 = 1$, so

$$X = \{x\}, \qquad R = \{(x^3)^k \mid k \in \mathbb{Z}\} \subset F_1 = \{x^k \mid k \in \mathbb{Z}\}.$$

Here the cosets of F_1/R are R, xR, x^2R. The set of these three cosets is closed under multiplication. For example, $(xR)(x^2R) = x(Rx^2)R = xx^2RR = x^3R = R$, so the inverse of the element xR is x^2R.

More generally, C_n has presentation

$$C_n = \{x \mid x^n = 1\}.$$

Exercise 9.3.1. By constructing moves of the Rubik's cube of order 2, 3, 4, show that the Rubik's cube "contains" the subgroups C_2, C_3, C_4.

Lemma 196. *The group $C_m \times C_n$ is presented by*

$$C_m \times C_n = \{a, b \mid a^m = 1, b^n = 1, ab = ba\}.$$

Remark 18. In general, if G is generated by g_1, ..., g_m with relations $R_i(g_1, ..., g_m) = 1$ and if H is generated by h_1, ..., h_n with relations $S_i(h_1, ..., h_n) = 1$ then $G \times H$ is the group generated by the g_i, h_j, with relations $R_i(g_1, ..., g_m) = 1$, $S_i(h_1, ..., h_n) = 1$, and $g_i h_j = h_j g_i$. We shall not prove this but refer to [MKS], Exercise 13, §4.1.

Exercise 9.3.2. By constructing moves of the Rubik's cube of order 2, 3 *which commute* show that the Rubik's cube "contains" the subgroups $C_2 \times C_3 \cong C_6$.

We conclude this section with a table of all the finite groups of order less than or equal to 25 and their generators and relations.

9.4 Generators, relations for groups of order < 26

The following table was obtained from the tables in [TW].

Notation:

C_n = cyclic group of order n,
D_n = dihedral group of order $2n$
= symmetry group of the regular n-gon,
Q = quaternion group = $\{-1, 1, -i, i, -j, j, -k, k\}$,
S_n = symmetric group of permutations of $\{1, 2, ..., n\}$,
A_n = alternating group of even permutations of $\{1, 2, ..., n\}$,
$\mathbb{F}_q$ = finite field with q elements (q=power of a prime),
$\mathbb{Z}/n\mathbb{Z}$ = integers modulo n.

Order	Group G	generators	relations	notes
2	C_2	a	$a^2 = 1$	
3	C_3	a	$a^3 = 1$	$G = A_3$
4	C_4	a	$a^4 = 1$	
4	$C_2 \times C_2$	a, b	$a^2 = 1, b^2 = 1,$ $ab = ba$	Klein 4-group $Aut(G) = GL(2, \mathbb{F}_2)$
5	C_5	a	$a^5 = 1$	
6	$C_6 = C_2 \times C_3$	a	$a^6 = 1$	
6	S_3	a, b	$a^3 = 1, b^2 = 1,$ $aba = b$	$Aut(G) = G$ $G = GL(2, \mathbb{F}_2)$
7	C_7	a	$a^7 = 1$	
8	C_8	a	$a^8 = 1$	
8	$C_2 \times C_4$	a, b	$a^2 = 1, b^4 = 1,$	
			$ab = ba$	
8	$C_2 \times C_2 \times C_2$	a, b, c	$a^2 = 1, b^2 = 1,$ $c^2 = 1, ab = ba,$ $bc = cb, ac = ca$	$Aut(G) = GL(3, \mathbb{F}_2)$
8	D_4	a, b	$a^4 = 1, b^2 = 1,$ $aba = b$	
8	Q	a, b	$a^4 = 1, b^2 = a^2,$ $aba = b$	
9	C_9	a	$a^9 = 1$	
9	$C_3 \times C_3$	a, b	$a^3 = 1, b^3 = 1,$ $ab = ba$	$Aut(G) = GL(2, \mathbb{F}_3)$
10	$C_{10} = C_2 \times C_5$	a	$a^{10} = 1$	
10	D_5	a, b	$a^5 = 1, b^2 = 1,$ $aba = b$	
11	C_{11}	a	$a^{11} = 1$	
12	$C_{12} = C_3 \times C_4$	a	$a^{12} = 1$	
12	$C_2 \times C_6$ $= C_2 \times C_2 \times C_3$	a, b	$a^2 = 1, b^6 = 1,$ $ab = ba$	
12	D_6	a, b	$a^6 = 1, b^2 = 1,$ $aba = b$	
12	A_4	a, b	$a^2 = 1, b^3 = 1,$ $(ba)^3 = 1$	$Aut(G) = G$
12	Q_6	a, b	$a^6 = 1, b^2 = a^3,$ $aba = b$	"dicyclic"

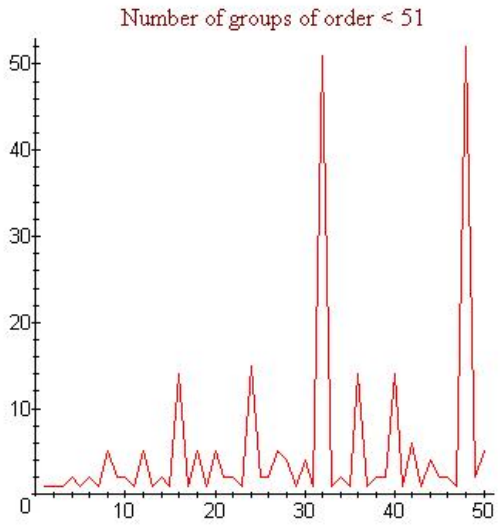
13	C_{13}	a	$a^{13}=1$	
14	$C_{14}=C_2\times C_7$	a	$a^{14}=1$	
14	D_7	a,b	$a^7=1, b^2=1,$ $aba=b$	$Aut(G)=G$
15	$C_{15}=C_3\times C_5$	a	$a^{15}=1$	
16	C_{16}	a	$a^{16}=1$	
16	$C_2\times C_8$	a,b	$a^2=1, b^8=1,$ $ab=ba$	
16	$C_4\times C_4$	a,b	$a^4=1, b^4=1,$ $ab=ba$	$Aut(G)=GL(2,\mathbb{Z}/4\mathbb{Z})$
16	$C_2^2\times C_4$	a,b,c	$a^2=1, b^2=1, c^2=1,$ $ab=ba, ac=ca, bc=cb$	
16	C_2^4	a,b,c,d	$a^2=1, b^2=1,$ $c^2=1, d^2=1,$ $ab=ba, ac=ca, ad=da,$ $bc=cb, bd=db, cd=dc$	$Aut(G)=GL(4,\mathbb{F}_2)$
16	$D_4\times C_2$	a,b,c	$a^4=1, b^2=1, c^2=1,$ $aba=b, ac=ca, bc=cb$	
16	$Q\times C_2$	a,b,c	Exercise	
16		a,b,c	$a^2=1, b^2=1, c^2=1,$ $abc=bca=cab$	
16		a,b	$a^2=1, b^2=1,$ $(ab)^2=1, (a^{-1}b)^2=1$	
16		a,b	$a^4=1, b^4=1,$ $aba=b$	a semidirect product of C_4 with C_4
16		a,b	$a^8=1, b^2=1,$ $ab=ba^5$	a semidirect product of C_8 with C_2 (C_2 normal)
16		a,b	$a^8=1, b^2=1,$ $ab=ba^3$	a semidirect product of C_8 with C_2 (C_2 normal)
16	D_8	a,b	$a^8=1, b^2=1,$ $aba=b$	a semidirect product of C_8 with C_2 (C_2 normal)
16	Q_8	a,b	$a^8=1, b^2=a^4,$ $aba=b$	
17	C_{17}	a	$a^{17}=1$	
18	$C_{18}=C_2\times C_9$	a	$a^{18}=1$	

18	$C_3 \times C_6$ $= C_3 \times C_3 \times C_2$	a, b	$a^3 = 1, b^6 = 1,$ $ab = ba$	
18	$S_3 \times C_3$	a, b, c	$a^3 = 1, b^2 = 1, c^3 = 1$ $aba = b, ac = ca, bc = cb$	
18	D_9	a, b	$a^9 = 1, b^2 = 1,$ $aba = b$	a semidirect product of C_9 with C_2 (C_2 normal), $Aut(G) = G$
18		a, b, c	$a^3 = 1, b^3 = 1, c^2 = 1$ $ab = ba, aca = c, bcb = c$	
19	C_{19}	a	$a^{19} = 1$	
20	$C_{20} = C_4 \times C_5$	a	$a^{20} = 1$	
20	$C_2 \times C_{10}$	a, b	$a^2 = 1, b^{10} = 1,$ $ab = ba$	
20	D_{10}	a, b	$a^{10} = 1, b^2 = 1,$ $aba = b$	
20	Q_{10}	a, b	$a^{10} = 1, b^2 = a^5,$ $aba = b$	
20		a, b	$a^5 = 1, b^4 = 1,$ $ab = ba^3$	a semidirect product of C_5 with C_4 (C_4 normal), $Aut(G) = G$
21	$C_{21} = C_3 \times C_7$	a	$a^{21} = 1$	
21		a, b	$a^7 = 1, b^3 = 1,$ $ab = ba^4$	a semidirect product of C_7 with C_3 (C_3 normal), $Aut(G) = G$
22	$C_{22} = C_2 \times C_{11}$	a	$a^{22} = 1$	
22	D_{11}	a, b	$a^{11} = 1, b^2 = 1,$ $aba = b$	$Aut(G) = G$
23	C_{23}	a	$a^{23} = 1$	
24	$C_{24} = C_3 \times C_8$	a	$a^{24} = 1$	
24	$C_2 \times C_{12}$ $= C_2 \times C_3 \times C_4$	a, b	$a^2 = 1, b^{12} = 1,$ $ab = ba$	
24	$C_2^2 \times C_6$	a, b, c	$a^2 = 1, b^2 = 1, c^6 = 1,$ $ab = ba, ac = ca, bc = cb$	

24	$D_6 \times C_2$	a, b, c	$a^6 = 1, b^2 = 1, c^2 = 1,$ $aba = b, ac = ca, bc = cb$	
24	$A_4 \times C_2$	a, b, c	Exercise	
24	$Q_6 \times C_2$	a, b, c	Exercise	
24	$D_4 \times C_3$	a, b, c	Exercise	
24	$Q \times C_3$	a, b, c	Exercise	
24	$S_3 \times C_4$	a, b, c	Exercise	
24	D_{12}	a, b	$a^{12} = 1, b^2 = 1,$ $aba = b$	
24	Q_{12}	a, b	$a^{12} = 1, b^2 = a^6,$ $aba = b$	
24	S_4	a, b	$a^4 = 1, b^2 = 1,$ $(ab)^3 = 1$	$Aut(G) = G$
24	$SL(2, \mathbb{F}_3)$	a, b, c	$a^4 = 1, b^2 = a^2,$ $c^3 = 1, aba = b,$ $ac = cb, bc = cab$	$Aut(G) = Aut(Q)$ $= S_4,$ a semidirect product of Q with C_3 (C_3 normal)
24		a, b	$a^3 = 1, b^8 = 1,$ $aba = b$	a semidirect product of C_3 with C_8 (C_8 normal)
24		a, b, c	$a^3 = 1, b^4 = 1,$ $c^2 = 1, bcb = c, aba = b,$ $ac = ca$	a semidirect product of C_3 with D_4 (D_4 normal)
25	C_{25}	a	$a^{25} = 1$	
25	C_5^2	a, b	Exercise	

Problem Which of these is (isomorphic to) a subgroup of the Rubik's cube group?

Problem Of those which are subgroups, find moves associated to the generators given which satisfy the relations given.



9.5 The presentation problem

The following problem is unsolved:

Problem (Singmaster [Si]): Let G be the Rubik's cube group. Find a set of generators and relations for G of minimal cardinality (i.e., $|X| + |Y|$ is of minimal cardinality).

Problem : Find

(a) a set of generators for G of minimal cardinality,

(b) a set of relations for G of minimal cardinality,

(c) an expression for each such generator as a word in the basic moves R, L, U, D, F, B.

The part (a) is known: there are 2 elements which generate G [Si]. Part (b) is not known (though Dan Hoey's post of Dec 17, 1995 to the cube-lover's list may describe the best known results [CL]; he suggests that G has a set X of 5 generators and a set Y of 44 relations such that the total length of all the reduced words in Y is 605).

9.5.1 A presentation for $C_m^n \wr\!\!\lhd S_{n+1}$

We begin an assault on the problem of D. Singmaster mentioned above. This section was written with Dennis Spellman.

We can identify the $C_m^n \wr\!\!\lhd S_{n+1}$ with the group of $(n+1) \times (n+1)$ invertible monomial matrices g with coefficients in C_m having the following condition on the determinant: if we write $g = p \cdot d$, where p is a permutation matrix and d is a diagonal matrix then $\det(d) = 1$ (this determinant 1 condition is a condition corresponding to the "conservation of twists" for the moves of the Rubik's cube).

We may identify C_m^n with the subgroup

$$\{(x_1, ..., x_{n+1}) \mid x_1 x_2 ... x_{n+1} = 1,\ x_i \in C_m\}$$

and $C_m^n \wr\!\!\lhd S_{n+1}$ as a subgroup of the wreath product $S_{n+1}\ wr\ C_m$.

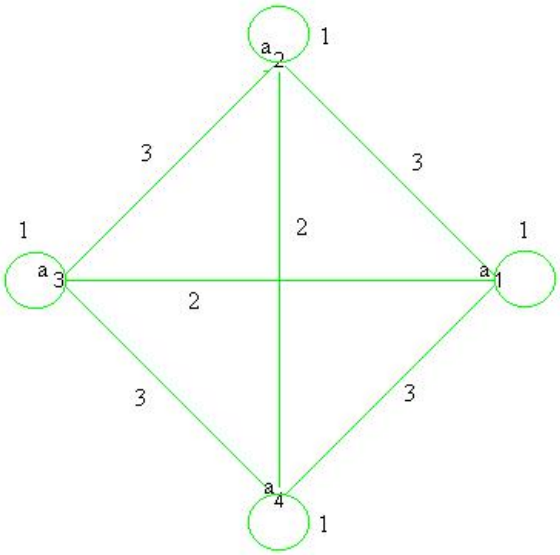
Consider $G = C_m^{n+1} \wr\!\!\lhd S_{n+1}$. The group S_{n+1} has presentation

$$S_{n+1} =< a_1, ..., a_n \mid (a_i a_j)^{m_{ij}} = 1,\ \forall 1 \le i, j \le n >,$$

where

$$m_{ij} = \begin{cases} 3, & j = i \pm 1, \\ 2, & |i - j| > 1, \\ 1, & i = j. \end{cases}$$

The following diagram may help to visualize the exponents m_{ij} in the case $n = 4$:



As a group of $(n+1) \times (n+1)$ monomial matrices, we identify a_i with the permutation matrix,

$$s_i = \begin{pmatrix} 1 & 0 & & & ... & & & 0 \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ 0 & ... & & & & & 0 & 1 \end{pmatrix}.$$

If I is the $(n+1) \times (n+1)$ identity matrix and if E_{ij} denotes the matrix which is 0 in every entry except the ij entry, which is 1, then

$$s_i = I - E_{ii} - E_{i+1,i+1} + E_{i,i+1} + E_{i+1,i}.$$

The group C_m has presentation

$$C_m = < h \mid h^m = 1 > .$$

The group C_m^n has presentation

$$C_m^n = < h_1, ..., h_n \mid h_i^m = 1,\ h_i h_j = h_j h_i, \forall 1 \leq i, j \leq n+1 > .$$

We identify C_m^n with the Cartesian product

$$\{(h_1(x_1), h_2(x_2), ..., h_n(x_n)) \mid x_i \in C_m\},$$

where $h_i(t)$ is the diagonal matrix

$$h_i(t) = I - E_{ii} - E_{i+1,i+1} + tE_{i,i} + t^{-1}E_{i+1,i+1}.$$

There are the following identities between the s_i and the $h_j(t)$:

$$\begin{gathered} s_i h_j(t) s_i^{-1} = h_j(t), \quad |i-j| > 1, \\ s_i h_i(t) s_i^{-1} = h_i(t)^{-1}, \\ s_{i\pm1} h_j(t) s_{i\pm1}^{-1} = h_i(t) h_{i\pm1}(t). \end{gathered}$$

This in mind motivates the formulation of the following statement (which we shall prove in the next section):

Theorem 197.

$$C_m^n \wr S_{n+1} =< a_1, ..., a_n, h_1, ..., h_n \mid \begin{array}{c} (a_i a_j)^{m_{ij}} = 1, \\ \forall 1 \leq i, j \leq n, \\ h_i^m = 1,\ h_i h_j = h_j h_i, \forall 1 \leq i, j \leq n \\ a_i h_j a_i^{-1} = h_j, \quad |i-j| > 1, \\ a_i h_i a_i^{-1} = h_i^{-1}, \\ a_{i\pm 1} h_j a_{i\pm 1}^{-1} = h_i h_{i\pm 1} > \end{array}$$

Remark 19. The above result was proven before it was noticed that essentially the same presentation may be found in the paper [DM] by Davies and Morris (where the group $C_m^n \wr S_{n+1}$ is called a generalized symmetric group).

9.5.2 Proof

Let P denote the group presented in the above theorem. The claim is, of course, that $C_m^n \wr S_{n+1} \cong P$. There is a surjective homomorphism $f : P \to C_m^n \wr S_{n+1}$ given by sending the generators to the generators. The problem is to which that this is injective. Let $K = ker(f)$, so

$$|P| = |P/K||K| \geq |P/K| = |C_m^n \wr S_{n+1}| = m^n(n+1)!.$$

Note $H =< h_1, ..., h_n \mid h_i^m = 1, h_i h_j = h_j h_i > <\ P$ is a normal subgroup of P since each a_i sends a generator of H to a product of them or their inverses. Also, note $H \cong C_m^n$.

We claim that $P/H \cong S_{n+1}$. From this it will follow that $|P| = m^n(n+1)!$, proving that $|K| = 1$, as desired.

To establish $P/H \cong S_{n+1}$, we show that the presentation on P/H one gets from Theorem 2.1 in [MKS] is the same as that of S_{n+1}. This is actually easy to see: If $W(a_1, ..., a_n, h_1, ..., h_n) = 1$ is a relation in the presentation, we must determine the word $W(a_1, ..., a_n, h_1, ..., h_n)H$ in P/H. Note that every relation "collapses" and becomes trivial except for the relations $(a_i a_j)^{m_{ij}} = 1$. These relations define the presentation for S_{n+1}, as desired. □

Chapter 10

The 3×3 Rubik's cube group

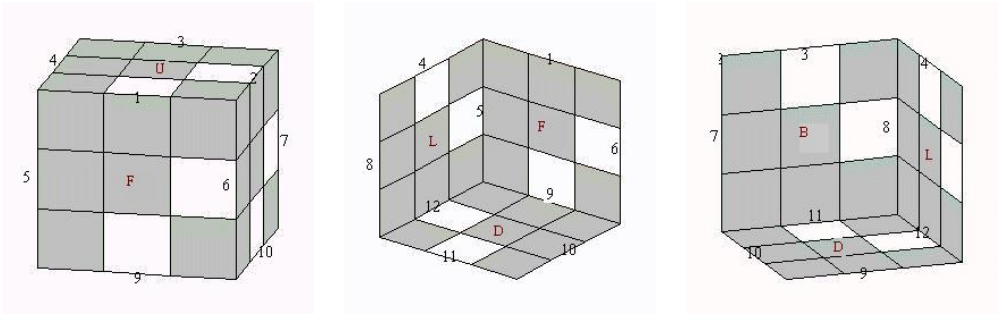
In this chapter, we describe mathematically the moves of the 3×3 Rubik's cube.

10.1 Mathematical description of the 3×3 cube moves

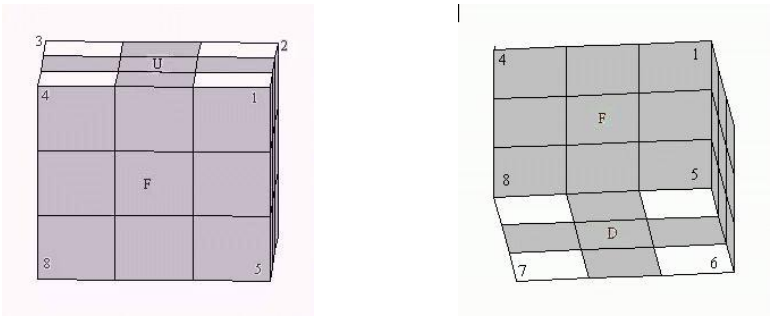
In this section, we describe mathematically the moves of the 3×3 Rubik's cube. As we will see, this will lead eventually to the description of the Rubik's cube group as a subgroup of index 12 of a direct product of two wreath products.

10.1.1 Notation

First, orient all the corners and edges as in theorem 60. These are depicted as follows, except that we have replaced the "+" in theorem 60 with a white square:



and



Let $G =< R, L, U, D, F, B >$ be the group of the 3×3 Rubik's cube and let H be the "enlarged" group generated by R, L, U, D, F, B and all the "illegal" moves (where one is allowed to disassemble and reassemble the cube but not remove any facets). Let V denote the set of vertices of the cube (which we identity with the set of corner subcubes of the Rubik's cube) and let

$$\rho : H \to S_V$$

denote the homomorphism which associates to each move of the Rubik's cube the cooresponding permutation of the vertices. Let E denote the set of edges of the cube (which we identity with the set of edge subcubes of the Rubik's cube) and let

$$\sigma : H \to S_E$$

denote the homomorphism which associates to each move of the Rubik's cube the corresponding permutation of the edges.

10.1.2 Corner orientations

Let $v : H \to C_3^8$ be the function which associates to each move $g \in H$ the corresponding corner orientations. More precisely, let $g \in H$ and say g moves corner i to corner j. Then $v_i(g) \in C_3$ is the orientation which the i^{th} vertex gets sent to by g, where the vertices are labeled as in the diagram shown and where the orientation is the number of 120^o clockwise twists required to turn the relative reference "+" obtained by moving corner i to j using the move g into the standard reference "+" on corner j.

Example 198. We have

X	$\vec{v}(X)$
F	(2,0,0,1,1,0,0,2)
U	(0,0,0,0,0,0,0,0)
F*U	(2,0,0,1,1,0,0,2)
U*F	(2,0,0,1,1,0,0,2)
D	(0,0,0,0,0,0,0,0)
B	(0,1,2,0,0,2,1,0)
R	(1,2,0,0,2,1,0,0)
L	(0,0,1,2,0,0,2,1)

Remark 20. The effect of a move $g \in H$ on the corner orientations may also be regarded as a relabeling of the "+" markings.

Note that a move $g \in H$ has two effects on the corners:
(a) a permutation $\rho(g) \in S_V$ of the vertices,
(b) a reorientation of the vertices moves in (a).
In particular, for $g, h \in H$, the orientation $\vec{v}(gh)$ can only differ from $v(g)$ in the coordinates corresponding to the vertices permuted by h.

We shall now verify that the "relative" orientation $\vec{v}(gh) - \vec{v}(g)$ is the same as the orientation $\vec{v}(h)$, provided one takes into account the effect of g on the vertices: $\vec{v}(h) = \rho(g)(\vec{v}(gh) - \vec{v}(g))$, i.e.,

Lemma 199. $\vec{v}(gh) = \vec{v}(g) + \rho(g)^{-1}(\vec{v}(h))$.

proof: The move gh orients the i^{th} corner subcube by $v_i(gh)$ and permutes the vertices by $\rho(gh)$, by definition.

On the other hand, gh will first act by g then h. The move g will reorient the i^{th} corner subcube by $v_i(g)$ and send the i^{th} vertex to the $\rho(g)(i)^{th}$ vertex.

To study the subsequent effect of h on this, let us subtract $\vec{v}(g)$ from $\vec{v}(gh)$, so that we are back to our original orientation (we will add $\vec{v}(g)$ back in later). Call this position the modified cube for now.

The move h first orients the j^{th} corner subcube of the modified cube by $v_j(h)$ and permutes it to vertex $\rho(h)(j)$. The i^{th} subcube of the modified cube comes from (via g) the $\rho(g)^{-1}(i)^{th}$ subcube of the original cube. Thus the i^{th} corner subcube of the modified cube is, by means of h, reoriented by $v_{\rho(g)^{-1}(i)}(h)$. To this we must add in $v_i(g)$ to get the total effect of gh on the i^{th} vertex of the original:

$$v_i(gh) = v_i(g) + v_{\rho(g)^{-1}(i)}(h)),$$

for each $1 \leq i \leq 8$, which implies Lemma 199. $\square$

10.1.3 Edge orientations

Let $w : H \to C_2^{12}$ be the function which associates to each move $g \in H$ the corresponding corner orientations. More precisely, let $g \in H$ and say g moves corner i to corner j. Then $w_i(g) \in C_2$ is the orientation which the i^{th} vertex gets sent to by g, where the vertices are labeled as in the diagram shown and where the orientation is the number of 180^o flips required to turn the relative reference "+" obtained by moving corner i to j using the move g into the standard reference "+" on corner j.

Example 200. We have

X	$\vec{w}(X)$
F	(1,0,0,0,0,0,0,0,1,0,0,0)
U	(1,0,1,0,0,0,0,0,0,0,0,0)
F*U	(1,0,1,0,1,0,0,0,1,0,0,0)
U*F	(1,1,1,0,0,0,0,0,1,0,0,0)
B	(0,0,0,0,0,0,1,1,0,0,0,0)
D	(0,0,0,0,0,0,0,0,0,1,0,1)
R	(0,1,0,0,0,1,1,0,0,1,0,0)
L	(0,0,0,0,1,0,0,0,1,0,0,0)

Remark 21. The effect of a move $g \in H$ on the edge orientations may also be regarded as a relabeling of the "+" markings.

Note that a move $g \in H$ has two effects on the edges:
(a) a permutation $\sigma(g) \in S_E$ of the edges,
(b) a reorientation of the edges which were moved in (a).
In particular, for $g, h \in H$, the orientation $\vec{w}(gh)$ can only differ from $\vec{w}(g)$ in the coordinates corresponding to the edges permuted by h.

We shall now claim that

$$\vec{w}(gh) = \vec{w}(g) + \sigma(g)^{-1}(\vec{w}(h)), \tag{10.1}$$

i.e., that

$$w_i(gh) = w_i(g) + w_{\sigma(g)^{-1}(i)}(h),$$

for each $1 \leq i \leq 12$. The proof of this is so similar to the proof of Lemma 199 that we leave it to the student to modify its proof to verify (10.1).

10.1.4 The semi-direct product

Consider the following direct product of two semi-direct products:

$$H' = (C_3^8 \ {>\!\!\lhd}\ S_V) \times (C_2^{12} \ {>\!\!\lhd}\ S_E).$$

Remark 22. This may also we written in the notation of wreath products as the following direct product of two wreath products:

$$H' = (S_V \text{ wr } C_3^8) \times (S_E \text{ wr } C_2^{12}).$$

As a *set*, we think of H as belonging to $C_3^8 \times S_V \times C_3^8 \times S_V$. If we represent elements h, h' of H as $h = (v, r, w, s), h' = (v', r', w', s') \in C_3^8 \times S_V \times C_3^8 \times S_V$ then the group operation will be given by

$$h * h' = (v, r, w, s) * (v', r', w', s') = (v + P(r)(v'), rr', w + P(s)(w'), ss').$$

Consider the function

$$\begin{array}{ccc} \iota : H & \to & (C_3^8 \ {>\!\!\lhd}\ S_V) \times (C_2^{12} \ {>\!\!\lhd}\ S_E) \\ g & \longmapsto & (v(g), \rho(g), w(g), \sigma(g)). \end{array}$$

Proposition 201. *ι is an isomorphism, $H \cong H'$.*

proof: Since

$$(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g)) * (\vec{v}(h), \rho(h), \vec{w}(h), \sigma(h))$$
$$= (\vec{v}(g) + P(\rho(g))(\vec{v}(h)), \rho(g)\rho(h), \vec{w}(g) + P(\sigma(g))(\vec{w}(h)), \sigma(g)\sigma(h)),$$

the map ι is a homomorphism. Since any reorientation and permutation can be achieved by some illegal move, ι must be surjective. By theorem 60, the kernel of ι is trivial (this is just a fancy way of saying that if no subcube is permuted or reoriented then the cube doesn't change!). □

10.2 Second fundamental theorem of cube theory

First, some preliminaries. We identify, as in §10.1, each $g \in G$ with a 4-tuple

$$(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g)),$$

where

- $\rho(g)$ is the corresponding permutation of the set of vertices V of the cube,
- $\sigma(g)$ is the corresponding permutation of the set of edges E of the cube,
- $v(g), w(g)$ are "orientations" defined in §10.1.

Remark 23. Let S_n denote the symmetric group on n letters and identify S_V with S_8, S_E with S_{12}. By example 138, we know that
(a) $\rho : G \to S_8$ is a homomorphism,
(b) $\sigma : G \to S_{12}$ is a homomorphism.

Question: Given a 4-tuple (v, r, w, s), where r, s are permutations of the corners, resp. edges, as above and

$$v \in C_3^8, \qquad w \in C_2^{12},$$

what conditions on r, s, v, w insure that it corresponds to a possible position of the Rubik's cube?

The following result is, according to [BCG], due to Ann Scott.

Theorem 202. *(Second fundamental theorem of cube theory) A 4-tuple (v, r, w, s) as above ($r \in S_8$, $s \in S_{12}$, $v \in C_3^8$, $w \in C_2^{12}$) corresponds to a possible position of the Rubik's cube if and only if*

(a) $sgn(r) = sgn(s)$, ("equal parity as permutations")
(b) $v_1 + ... + v_8 \equiv 0 \pmod 3$, ("conservation of total twists")
(c) $w_1 + ... + w_{12} \equiv 0 \pmod 2$, ("conservation of total flips").

proof: First we prove the "only if" part. That is, we assume that $(v, r, w, s) \in S_V \times S_E \times C_3^8 \times C_2^{12}$ represents a (legally obtained!) position of the Rubik's cube. From this we want to prove (a)-(c).

Let $g \in G$ be the element which moves the Rubik's cube from the solved position to the position associated to this 4-tuple. Then $r = \rho(g)$ and $s = \sigma(g)$. We know that g may be written as a word in the basic moves R, L, U, D, F, B, say $g = X_1...X_k$, where each X_i is equal to one of the R, L, U, D, F, B. Observe that if X is any one of these basic moves then $sgn(\rho(X)) = sgn(\sigma(X))$. Since sgn, ρ, and σ are homomorphisms, it follows that

$$sgn(r) = sgn(\rho(g)) = \prod_{i=1}^{k} sgn(\rho(X_i)) = \prod_{i=1}^{k} sgn(\sigma(X_i)) = sgn(\sigma(X)) = sgn(s).$$

This proves (a).

We have verified (b) for the basic moves in example 198 above. Note that

(i) the conservation of twists condition in (b) is true for $(v_1, ..., v_8)$ if and only if it is true for any permutation $P(p)(v) = (v_{(1)p}, ..., v_{(8)p})$,

(ii) if $(v_1, .., v_8)$ and $(v'_1, ..., v'_8)$ each satisfy the conservation of twists condition in (b) then their sum also satisfies it.

As above, write g as a word in the basic moves R, L, U, D, F, B, say $g = X_1...X_k$, where each X_i is equal to one of the R, L, U, D, F, B. We assume that this expression is minimal in the sense that we choose the X_i so that k is as small as possible. This k is called the length of g. (This length is the same as the distance from g to the identity in the Cayley graph of G.)

We now prove (b) by induction on the length. We have already checked it for all words of length $k = 1$.

Assume $k > 1$. By the formula giving the orientation of the product of two moves in terms of the two orientations of the moves, we have

$$\vec{v}(X_1...X_{k-1}X_k) = \rho(X_1...X_{k-1})^{-1}(\vec{v}(X_k)) + \vec{v}(X_1...X_{k-1}).$$

The term $\rho(X_1...X_{k-1})^{-1}(\vec{v}(X_k))$ satisfies the conservation of twists condition in (b) by (i) above. The term $\vec{v}(X_1...X_k)$ satisfies the conservation of twists condition in (b) by the induction hypothesis. Their sum satisfies the conservation of twists condition in (b) by (ii) above. This proves (b).

The proof of (c) is very similar to the proof of (b), except that we use example 200 in place of example 198.

Exercise 10.2.1. Provide the details.

Now, we must prove the theorem in the "if" direction. In other words, assuming (a), (b), and (c) we must show that there is a corresponding legal position of the Rubik's cube. This part of the proof is constructive.

First, we prove a special case. Assume that r and s are both the identity and that $(w_1, ..., w_{12}) = (0, ..., 0)$.

There is a move which twists exactly two corners and preserves the orientations and positions of all other subcubes. For example, the move $g = (R^{-1}D^2RB^{-1}U^2B)^2$ twists the ufr corner by 120^o clockwise, the bdl corner by 240^o clockwise, and preserves the orientations and positions of all other subcubes. This move can be easily modified, by a suitable conjugation, to obtain a move which twists any pair of corners, and preserves the orientations and positions of all other subcubes. These moves generate all possible 8-tuples satisfying the conservation of twists condition in (b). This proves the "if" part of the theorem in the case that r and s are both the identity and that $(w_1, ..., w_{12}) = (0, ..., 0)$.

Next, we prove another special case. Assume that r and s are both the identity and that $(v_1, ..., v_8) = (0, ..., 0)$.

There is a move which flips exactly two edges and preserves the orientations and positions of all other subcubes. For example, the move $g = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$ (found in [B], page 112) flips the uf edge, the ur edge, and preserves the orientations and positions of all other subcubes. This move can be easily modified, by a suitable conjugation, to obtain a move which flips any pair of edges, and preserves the orientations and positions of all other subcubes. These moves generate all possible 12-tuples satisfying the conservation of flips condition in (c). This proves the "if" part of the theorem in the case that r and s are both the identity and that $(v_1, ..., v_8) = (0, ..., 0)$.

As a consequence of these last two special cases, it follows that the "if" part of the theorem is true in the case that r and s are both the identity.

Finally, we prove our last special case. Assume that $(v_1, ..., v_8) = (0, ..., 0)$ and that $(w_1, ..., w_{12}) = (0, ..., 0)$. Consider the following three claims.

- Given any three edges subcubes, there is a move which is a 3-cycle on these edges and preserves the orientations and positions of all other subcubes.
- Given any three corners, there is a move which is a 3-cycle on these corners and preserves the orientations and positions of all other subcubes.
- Given any pair of edges and any pair of corners, there is a move which is a 2-cycle on these edges, a 2-cycle on these corners, and preserves the orientations and positions of all other subcubes.

Exercise 10.2.2. Verify these three claims.

By proposition 159, we know that A_E is generated by the edge 3-cycles above and that A_V is generated by the corner 3-cycles above. In other words, we can construct a position of the Rubik's cube associated to any 4-tuple $(r, s, 0, 0)$, provided $r \in A_V$ and $s \in A_E$. The subgroup $A_E \times A_V$ is index 4 in $S_E \times S_V$ since $|S_n/A_n| = 2$. The third type of move, the edge-corner 2-cycles above, does not correspond to an element of the subset $A_E \times A_V$ of the Rubik's cube group because an edge 2-cycle is an odd permutation of the edges. Therefore, if we consider the subgroup of $S_E \times S_V$ generated by all three types of moves we will obtain either all of $S_E \times S_V$ or some subgroup of index 2 which properly contains $A_E \times A_V$. The first possibility can be ruled out since it contradicts the parity condition in (a). The only subgroup of $S_E \times S_V$ of index 2 which properly contains $A_E \times A_V$ is the subgroup of elements satisfying the parity condition in (a).

It follows that the "if" part of the theorem is true in the case that v and w are both zero.

The theorem is a consequence of these special cases because of the following

Claim: There is always a move, no matter what position of the Rubik's cube is in, which does not permute any subcubes but "solves" the orientation of the cube so that v and w are both zero.

Exercise 10.2.3. Prove this claim.

□

Corollary 203. $G = \{g = (v, r, w, s) \in H \mid (a), (b), (c)$ in the above theorem hold$\}$.

10.2.1 Some consequences

We shall now reformulate the above fact about the Rubik's cube group from a point of view which (to me anyway) allows us to count the number of elements it has easier. Let

$$\begin{gathered} G_0 = \{(v, r, w, s) \mid r \in S_8,\ s \in S_{12}, \\ v = (v_1, v_2, ..., v_8), v_i \in \{0, 1, 2\}, v_1 + ... + v_8 \equiv 0 \pmod 3, \\ w = (w_1, w_2, ..., w_{12}), w_i \in \{0, 1\}, w_1 + ... + w_{12} \equiv 0 \pmod 2\}. \end{gathered}$$

Define a binary operation $* : G_0 \times G_0 \to G_0$ by

$$(v, r, w, s) * (v', r', w', s') = (v + P(r)(v'), r * r', w + P(s)(w'), s * s').$$

This defines a group structure on G_0. This is a subgroup of the enlarged Rubik's cube group of index 6.

Theorem 204. *There is an isomorphism*

$$G_0 \cong (C_3^7 >\!\lhd S_8) \times (C_2^{11} >\!\lhd S_{12}),$$

where C_n is the cyclic group with n elements and $>\!\lhd$ denotes the semi-direct product and where C_n^k ($n = 2, 3$, $k = 7, 11$) is identified with the subgroup of C_n^{k+1} defined by

$$\{v = (v_1, v_2, ..., v_k) \mid v_i \in \{0, 1, n-1\}, v_1 + ... + v_k \equiv 0 \pmod n\}.$$

In particular,

$$|G_0| = |S_8||S_{12}||C_2^{11}||C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7.$$

Theorem 205. *The Rubik's cube group G is the kernel of the homomorphism*

$$\begin{gathered} \phi : G_0 \to \{1, -1\} \\ (v, r, w, s) \longmapsto sgn(r)sgn(s). \end{gathered}$$

In particular, $G < G_0$ is normal of index 2 and

$$|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7.$$

Recall that the commutator subgroup G_1 of G is the subgroup consisting of all finite products of commutators

$$[g, h] = g * h * g^{-1} * h^{-1},$$

where g, h are arbitary elements of G.

Theorem 206. $|G_1| = |G|/2$.

In fact, we can explicitly determine G_1.

Theorem 207. $G_1 = \{g \in G \mid sgn(\rho(g)) = sgn(\sigma(g)) = 1\}$.

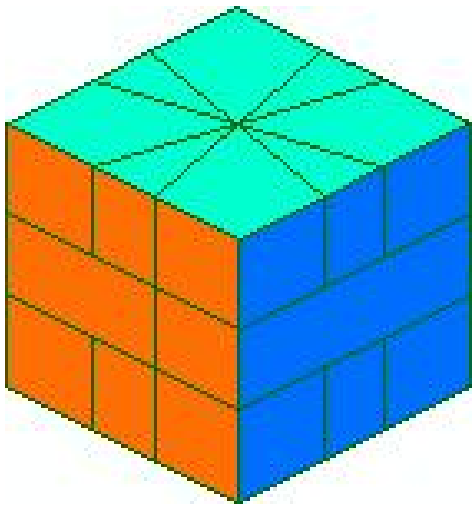
This basically follows from the fact that the commutator subgroup of S_n is A_n, for $n > 4$ (see chapter 3 of [R]; in fact, for $n > 4$, A_n is the only proper non-trivial normal subgroup of S_n).

The above theorem implies that $|G/G_1| = 2$ (to see this, use the first homomorphism theorem). From this, it clearly follows (from those who see it clearly) that G_1 is a normal subgroup of G.

10.3 The homology group of the square 1 puzzle

This section is based on a paper written jointly with J. McShea [JM].

Here we study the group theoretic properties of the collection G of all "words" in the basic moves of the square 1 puzzle which preserve the cube shape. This collection G forms a group which, motivated by [W], we call the homology group of the square 1 puzzle. The list of shapes which the square 1 puzzle can make is given in [Sn2]. It is not hard to see that the homology group of any one of these other shapes is conjugate to G, so from a group-theoretic standpoint, we may focus our attention on the cube. We shall also make use of the moves given in [Are] which belong to G.



A bi-product of the proof is an collection of moves which can be used to solve the square 1 puzzle, once it is put in the cube shape.

10.3.1 The main result

Let S_n denote the symmetric group of degree n, i.e., the group of permutations of $\{1, 2, ..., n\}$. Let $sgn : S_n \to \{\pm 1\}$ denote the homomorphism which assigns to each permutation its sign (the sign of a cyclic permutation of length r is $(-1)^{r+1}$, for example).

We shall see that the size of the homology group of the square 1 is about .8 billion.

Theorem 208. *G is isomorphic to the kernel of index 2 in $S_8 \times S_8$ of the homomorphism $f : S_8 \times S_8 \to \{\pm 1\}$ defined by $f(g_1, g_2) = sgn(g_1)sgn(g_2)$. Consequently, $|G| = 2^{13}3^45^27^2 = 812851200$.*

As a corollary of the proof of this theorem, given below, we shall see that any even permutation of the corners is possible and any even permutation of the wedges is possible.

Let H denote the enlarged square 1 group generated by all legal moves preserving the cube shape and all illegal moves (i.e., disassembly and reassembly is allowed) preserving the cube shape. It is clear that

$$H \cong S_8 \times S_8.$$

Some notation

We shall assume that the puzzle is in the solved position with the "square 1" side in front, right-side up. Let

- u denote rotation of the up face by 30^o clockwise,
- d denote rotation of the up face by 30^o clockwise,
- R denote rotation of the cube by 180^o though one of the skew-diagonal cuts (in a given position, at most one such move is possible, so this is unambiguous).

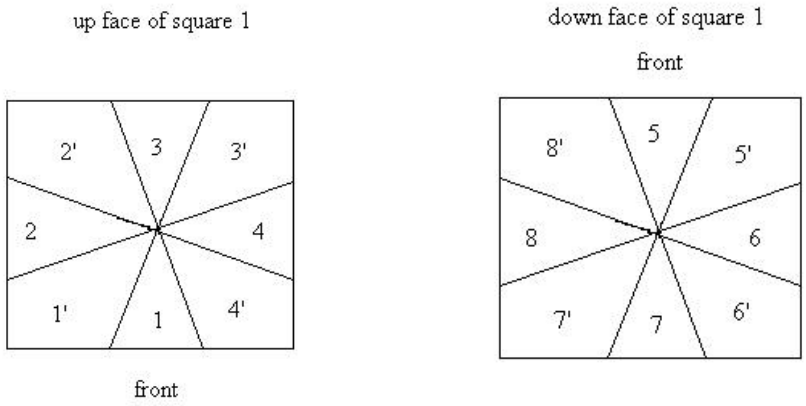
.

Like the 15 puzzle, and unlike the Rubik's cube, not any sequence of u, d, and R's is possible.

Let

$$T(x,y) = u * R * x * y * R * u^{-1}, B(x,y) = d^{-1} * R * x * y * R * d,$$

where x, y are moves of the square 1 puzzle.



In the notation of these diagrams, we have

$$uRu^{-1}d^{-1}Rd = (2,8)(4,6)$$
$$T(u^3,1) = (1',6',7',4')(1,6,7,4)$$
$$T(1,d^3) = (2',3',8',5')(2,3,8,5)$$
$$B(u^3,1) = (1,2,7,8)(1',6',7',4')$$
$$B(1,d^3) = (3,4,5,6)(2',3',8',5').$$

Two subgroups

Let

$$G_u =< T(u^3,1), T(1,d^3) >$$

and

$$G_d =< B(u^3,1), B(1,d^3) >$$

Lemma 209. *G_u and G_d are each isomorphic to $C_4 \times C_4$.*

proof: We have $T(u^3,1)T(1,d^3) = T(1,d^3)T(u^3,1)$. Moreover, $T(u^3,1)$ and $T(1,d^3)$ are each of order 4. Since

$$C_4 \times C_4 =< a,b \mid a^4 = 1, b^4 = 1, ab = ba >,$$

the lemma follows. □

The homology group of the square 1 puzzle is defined to be

$$G =< d^3, u^3, B(u^3,1), B(1,d^3), T(u^3,1), T(1,d^3) >$$

We shall use the following labelings to describe the moves of the square 1 puzzle

10.3.2 Proof of the theorem

We shall prove the theorem in the following steps:

- Show that the wedge 3-cycle $(1,2,3)$ and the corner 3-cycle $(1',2',3')$ each belong to G.
- Show that any wedge 3-cycle $(1,2,i)$ and each corner 3-cycle $(1',2',i')$ belong to G.
- Show that there is a injective homomorphism $\phi : G \to S_8 \times S_8$ where the image $\phi(G)$ contains $A_8 \times A_8$.
- Conclude that $G \cong S_8 \times S_8/\{\pm 1\}$.

Step 1: First, we claim that $(1,2,3)$ belongs to G. In fact, the 3-cycle $(1,2,3)$ is obtained from the move

$$M_1 = (B(u^3,1)*d^3)*((B(u^3,1)*d^{-3})*(B(u^{-3},1)*T(1,d^{-3})*d^6)))^4*(B(u^3,1)*d^3)^{-1}.$$

(Incidently, this 80 move long manuever may be verified using GAP [Gap]. See also [Sn2].)

Next, we claim that $(1',2',3')$ belongs to G. In fact,

$$M_2 = Ru^3Rd^{-3}Ru^3(Ru^{-3})^2d^3Ru^{-3}$$

is the product of 2-cycles $(2',3')(3,4)$. (This move was found in [Sn2].) Therefore, $u^3M_2u^{-3}$ is the product of 2-cycles $(1',2')(2,3)$. The product of these

is $(1', 2', 3')(2, 3, 4)$. Since $(2, 3, 4)$ is obtained from $u^{-3}M_1u^3$, we see that $(1', 2', 3')$ is in G. (This may also be verified using GAP.)

Step 2: Let g be any move in G which sends wedges 3 to wedge i, resp., and does not move wedges $1, 2$ (it may permute other wedges and corners). Then $(1, 2, i) = g * (1, 2, 3) * g^{-1}$. Thus $(1, 2, i) \in G$.

The proof that each $(1', 2', i') \in G$ is similar.

Step 3: It is clear from our definition that there is an injection $G \to S_8 \times S_8$ *as sets*. The verification that this is a homomorphism is straightforward.

Step 4: The group A_8 is generated by the 3-cycles $(1, 2, i)$ (see Lemma 160). Since these all belong to G, all even wedge permutations are possible. Similarly, all even corner permutations are possible. Thus $A_8 \times A_8 \subset G$.

Let $p_1 : S_8 \times S_8 \to S_8$ denote the projection onto the first factor. Let p_2 denote the projection onto the second factor. For each generator $g \in \{d^3, u^3, B(u^3, 1),\ B(1, d^3), T(u^3, 1), T(1, d^3)\}$ of G we have $sgn(p_1(g)) = sgn(p_2(g))$. Thus the image $\phi(G)$ is strictly contained in $S_8 \times S_8$. In fact, this shows that $\phi(G)$ is contained in the kernel $ker(f)$ of the homomorphism $f : S_8 \times S_8 \to \{\pm 1\}$ defined in the statement of the theorem. Since

$$A_8 \times A_8 \subset G \subset ker(f),$$

$[ker(f) : A_8 \times A_8] = 2$, and $T(u^3, 1) \notin A_8 \times A_8$, the theorem follows. $\square$

Chapter 11

Other Rubik-like puzzle groups

> "An expert is someone who knows some of the worst mistakes that can be made in his subject, and how to avoid them."
> *Heisenberg, Werner*
> *PHYSICS AND BEYOND, 1971*

This chapter shall survey, sometimes without proofs, some results on the group-theoretical structure of some of the permutation puzzle groups, as discussed in [GT], [Lu], [B], chapter 2, [NST], chapter 19.

11.1 On the group structure of the skewb

This section is based on G. Gomes and J. Montague [GM].

Notation: We fix an orientation of the cube and label the sides by R, L, U, D, F, B as in the case of the Rubik's cube. The 120 degree clockwise rotation of a corner is denoted by a 3-letter juxtaposition of the letters abbreviating the 3 faces which the corner meets. (When you twist a corner of the skewb you must permute three other corners but the opposite side of the skewb is unaffected.) Such a move will be called a basic move - there are 8 of them, though twisting about a corner and twisting about the antipodal opposite corner is basically the same move (up to a rotation of the entire cube.) For example, FRU denotes the 120 degree clockwise rotation of the front-right-up corner, leaving the rest of the cube alone.

Let C denote the set of square center facets and V the set of vertices of the cube.

Let

$$G =< FRU, FLU, BRU, BLU, DFR, DFL, BDR, BDL >$$

denote the group of all (legal) skewb moves. Let G^* denote the group of all legal and "illegal moves" (where disassembly then reassembly is allowed).

On each square center facet of the skewb we may choose a vertex with the following property: if we draw an arrow pointing from the chosen vertex of the square to the diametically opposite vertex on the square then the moves of the skewb permute these arrows amongst themselves, except that some arrows may possibly be reversed. This determines an orientation of each center facet. Call this puzzle the super skewb. For this new puzzle, let

$$G_{super} =< FRU, FLU, BRU, BLU, DFR, DFL, BDR, BDL >$$

denote the group of all (legal) super skewb moves. Let G^*_{super} denote the group of all legal and "illegal moves" (where disassembly is allowed).

We orient the corners as in the case for the Rubik's cube. Let $y(g) \in C_3^8 = \{0, 1, 2\}^8$ denote the orientation for the corners.

For the superskewb, we orient the center facets similarly. Let $z(g) \in C_4^6 = \{0, 1, 2, 3\}^6$ denote the orientation for the centers.

Let S_C denote the symmetric group on the set C, S_V the symmetric group on the set V.

Claim: There are homomorphisms

$$\rho : G \to S_C, \qquad \sigma : G \to S_V,$$

given, for each move $g \in G$, by

$$\rho(g) = \text{permutation of the center facets associated to } g,$$

and

$$\sigma(g) = \text{permutation of the vertices associated to } g.$$

Let

$$H = C_3^8 \times S_C \times S_V$$

and define $* : H \times H \to H$ by

$$(y, r, s) * (y', r', s') = (rr', ss', r^{-1}(y') + y).$$

Let

$$H_{super} = C_3^8 \times S_V \times C_4^6 \times S_C$$

and define $* : H_{super} \times H_{super} \to H_{super}$ by

$$(y, r, z, s) * (y', r', z', s') = (r^{-1}(y') + y, rr', s^{-1}(z') + z, ss').$$

Observation: There is an embedding of G into H and an embedding of G_{super} into H_{super}.

Let G_C be the group that acts only on the center facets of the skewb, and G_V the group that acts only on the vertices. Now,

$$G = G_C \times G_V.$$

Every generator of G is a 3-cycle on the center facets. This means that r is an element of A_C. It is a fact that the elements (i, j, k) of S_n generate A_n (for i, j, k elements of $\{1, 2, ..., n\}$). Therefore, $G_C = A_6$.

The group that acts on the vertices of the skewb is slightly more complicated. Unlike the Rubik's cube, there is no condition like conservation of twists which applies to the entire vertex set. Instead, we must split the vertices of the skewb into two 4-corner orbits. This idea is borrowed from Bandelow's booklet on Mickey's Challenge (a puzzle similar to the skewb). An orbit is constructed by starting with one corner and including the opposite corner of each face that meets at the first corner. Referring back to our original labeling of the skewb, the orbits are the odd corners $\{1, 3, 5, 7\}$, and the even corners $\{2, 4, 6, 8\}$. Let the orbit of odd corners be denoted by $V(odd)$, and let $V(even)$ denote the orbit of even corners. We now partition G_V so that

$$G_V = G_{V(odd)} \times G_{V(even)}.$$

We know that each orbit maps to a permutation on 4 vertices and an orientation on 4 vertices. So

$$G_V \text{ is a subgroup of } (C_3^4 >\!\lhd S_4) \times (C_3^4 >\!\lhd S_4).$$

Let $h = (s, u(h), t, v(h))$ be an element of G_V.

First we will examine the permutations of the vertices of both orbits. Each generator produces a 3-cycle on the vertices, whether they are in the odd or even orbit. Therefore, we can say that the permutations of each orbit generate A_4 by the same argument used for the center permutations. Now,

$$G_V \text{ is a subgroup of } (C_3^4 >\!\lhd A_4) \times (C_3^4 >\!\lhd A_4).$$

Claim 1: There exist h, such that s is an element of A_4, $u(h) = (0, 0, 0, 0)$, t is an element of A_4, and $v(h) = (0, 0, 0, 0)$. We know this is true because there are clean skewb moves which only permute 3 vertices.

Claim 2: Given any permutation u' of $(1, 2, 0, 0)$ by an element of A_4 and any permutation v' of $(1, 2, 0, 0)$ by an element of A_4, there exist h, such that $s = 1$, $u(h) = u'$, $t = 1$, and $v(h) = v'$. This is true because there are clean skewb moves which only twist vertices.

If we combine the moves of Claims 1 and 2, we should generate all of the possible moves of G_V. The condition on each of the vertex 4-tuples will drop them in dimension to elements of C_3^3. So we can conclude that G_V is a subgroup of index 9 of

$$(C_3^4 >\!\lhd A_4) \times (C_3^4 >\!\lhd A_4).$$

Note: This claim is verified by GAP.

Since $G_C = A_6$, and $G_V = (C_3^3 >\!\lhd A_4) \times (C_3^3 >\!\lhd A_4)$, we can conclude that

$$G = A_6 \times (C_3^3 >\!\lhd A_4) \times (C_3^3 >\!\lhd A_4).$$

and

$$|G| = (6!/2) * (4!/2)^2 * (3^6) = 37,791,360.$$

In conclusion, it is interesting to note that if we let G' denote the illegal skewb group - where reassembly is permitted - then

$$G' = S_6 \times S_8 \times C_3^8.$$

and

$$|G|/|G'| = .0001984127...$$

This means that if you could take apart the skewb and reassemble it however you wanted (leaving the stickers intact however), then only about .02 percent of all possible reassemblies would be solvable. The analogous percentage for the Rubik's cube is 8.33.. percent. As M. Schönert points out in a post to [CL], this makes the skewb harder to solve that the Rubik's cube in some sense .

Permutation and Orientation Tables

Move	Center Permutation	Vertex Permutation
UFR	(1 5 2)	(2 6 4)
UFL	(1 4 5)	(1 7 3)
DFR	(1 2 6)	(1 5 7)
DFL	(1 6 4)	(4 6 8)
BRU	(2 5 3)	(1 3 5)
BLU	(3 5 4)	(2 4 8)
DBR	(2 3 6)	(2 8 6)
DBL	(3 4 6)	(3 7 5)

Move	Vertex Orientation
UFR	(1 2 0 2 0 2 0 0)
UFL	(2 0 2 1 0 0 2 0)
DFR	(2 0 0 0 2 1 2 0)
DFL	(0 0 0 2 0 2 1 2)
BRU	(2 1 2 0 2 0 0 0)
BLU	(0 2 1 2 0 0 0 2)
DBR	(0 2 0 0 1 2 0 2)
DBL	(0 0 2 0 2 0 2 1)
UFR*UFL	(0 2 2 2 0 0 2 0)
DFR*DFL	(2 0 0 2 0 0 2 2)

Note: The orientations for the generator moves contain two repeated orbits - permutations of (1 0 0 0) and permutations of (2 2 2 0).

11.2 Mathematical description of the 2×2 cube moves

This section, which is based on [DL], derives the group structure of the 2×2 Rubik's cube.

A position on the 2×2 cube is determined by
(a) a permutation of the vertices, and
(b) the orientation of the corner sub-cubes.
An illegal move on the 2×2 cube is a reassembly of the corners.
Let

$$H =< R, L, U, D, F, B, \text{ and all the illegal moves} > .$$

This will be called the enlarged 2×2 cube group. Let $G =< R, L, U, D, F, B >$. G is contained in H with $G < H$.

Let $C_3^8 = \{0, 1, 2\}^8$ be the group of 8-tuples with coordinate-wise addition mod 3. Let $v : H \to C_3^8$ be defined as follows: Assume $h \in H$ sends the i^{th} corner to the j^{th} corner. $v_i(h)$ is the number in $C_3 = \{0, 1, 2\}$ which describes the orientation that the standard reference marking of the i^{th} corner is sent to relative to the standard reference marking of the j^{th} corner. The values of v are tabulated in (198).

Let S_V be the group of permutation of corner sub-cubes. We may identify S_V with S_8 since we have labeled the corners $1, ..., 8$. H is a subset of the Cartesian product $S_V \times C_3^8$.

Let $p(h)$ denote the permutation of the vertices of the cube associated to $h \in H$. We have

$$\begin{gathered}(v, r) * (v', r') = (v + r(v'), r * r') \\ (\vec{v}(g), p(g)) * (\vec{v}(h), p(h)) = (\vec{v}(g) + p(g)\vec{v}(h), p(g) * p(h)) \\ = (\vec{v}(g * h), p(g * h)).\end{gathered}$$

It is not hard to show, based on the results of the previous section, that $H = C_3^8 >\lhd S_8 = \{(v, r) \mid r \in S_V,\ v \in C_3^8\}$. In other words, H is the wreath product of S_8 and C_3.

Theorem 210. *A two-tuple $(v, r) \in C_3^8 \times S_V$ corresponds to a legal position iff $v_1 + ... + v_8 \equiv 0 \pmod 3$ (conservation of twists).*

proof: PART 1: In this part, we show that any pair (v, r) as in the theorem (where v satisfies conservation of twists) corresponds to a legal move g in such a way that $r = \rho(g)$ and $v = \vec{v}(g)$.

Case 1: Assume $r = 1$ and v is arbitrary. From the solved position, any two corners, corner i and corner j say, can be twisted so that corner i has orientation 1, corner j has orientation 2, and all other corners have orientation 0. Call such a move $e_{i,j}$. Example: $(R^{-1} * D^2 * R * B^{-1} * U^2 * B)^2$ is $e_{2,7}$.

Let $y = a_1 * e_{1,8} + ... + a_7 * e_{7,8}$, where $a_i \in \{0, 1, 2\}$. This is a move of the 2×2 Rubik's cube of the form $(v, 1)$ - in other words, it permutes nothing but may twist some corners. By construction, all moves of this form are legal. For each $a_i * e_{i,8}$ there are three different possible positions (independent of all other $a_j * e_{j,8}$). Since there three choices for each a_i, there are a total of 3^7 distinct moves of the form y as above.

On the other hand, there are exactly 3^7 possible moves of the form $(v, 1)$ which satisfy the conservation of twists. (proof: If $v = (v_1, ..., v_8)$, $v_i \in \{0, 1, 2\}$, and $v_1 + ... + v_8 \equiv 0 \pmod 3$, then there are 3 ways to choose each of $v_1, .., v_7$ but then once these are fixed the consevation of twists condition leaves no choice for v_8. This leaves a total of 3^7 choices.) These 3^7 possible moves include, of course, the legal moves of the form y above. Thus every move of the form $(1, v)$, with v satisfying conservation of twists, is legal.

Case 2: Assume $v = \vec{0}$ and r is arbitrary. Recall S_8 is generated by the two-cycles (see chapter 3 above, §§3.3-3.4).

Claim 1: Given any pair of corners, there is a 2-cycle move which swaps them. (Example: $F^{-1} * U * B * U^{-1} * F * U^2 * B^{-1} * U * B * U^2 * B^{-1}$). Once two corners have been swapped, you may correct the orientation of any sub-cube by Case 1. Thus any permutation which preserves orientations is a legal moves.

Case 3: Assume v and r are both arbitrary but satisfying conservation of twists. By case 2, we may make a legal move that changes (v, r) to $(v, 1)$. By case 1, $(v, 1)$ is a legal move.

PART 2: In this part, we show that any legal move satisfies conservation of twists.

Assume $(v, r) \in C_3^8 \times S_V$ is a legal move.

Define the length of a move $g \in G$ to be the smallest number n of generators needed to create the move, written $length(g) = n$.

Induction hypothesis: If a move is length n, it satisfies conservation of twists.

step $n = 1$: Every $\vec{v}(x)$ where $x \in \{R, L, U, D, F, B\}$ satisfies the conservation of twists.

step $n > 1$: Assume the induction hypothesis is true for all lengths $\leq n-1$. Let x be length n and write $x = x_1 * x_2$, where $length(x_1) \leq n - 1$ and $length(x_2) = 1$. Then $\vec{v}(x) = \vec{v}(x_1) + p(x_1)\vec{v}(x_2)$, by the group operation. Furthermore, $v(x_1)$ satisfies conservation of twists by the induction hypothesis. Since $p(x_1)$ simply permutes the coordinates of $\vec{v}(x_2)$, $\vec{v}(x_2)$ still satisfies the conservation of twists. The sum of moves satisfying conservation of twists still satisfies conservation of twists.

Conclusion: by induction, any move $(v, r) \in C_3^8 \times S_V$ that is a legal move satisfies the conservation of twists. □

11.3 On the group structure of the pyraminx

The results of this section were worked out in A. Luers [Lu].

Notation: Let

- V denote the vertices of the tetrahedron (which we identify with the set of corner pieces of the pyraminx),
- E denote the edges of the tetrahedron (which we identify with the set of edge pieces of the pyraminx),
- C the set of interior pieces of the tetrahedon (ie, movable pieces of the pyraminx not in E or V),
- S_V the permutation group of V,
- A_V the alternating group of V,
- S_E the permutation group of E,
- A_E the alternating group of E.

Assume that the tetrahedron is lying on a flat surface in front of you, with the triangle base pointing away from you. The corners are denoted L (left), R (right), U (up), and B (back).

Basic Moves: Opposite each corner or vertex there are three layers: the tip, the middle layer, and the opposite face. Let

- l denote the 120 degree clockwise rotation of the tip containing the left corner,
- L denote the 120 degree clockwise rotation of the tip/middle layer containing the left corner,
- r denote the 120 degree clockwise rotation of the tip containing the right corner,
- R denote the 120 degree clockwise rotation of the tip/middle layer containing the right corner,
- u denote the 120 degree clockwise rotation of the tip containing the up corner,

- U denote the 120 degree clockwise rotation of the tip/middle layer containing the up corner,
- b denote the 120 degree clockwise rotation of the tip containing the back corner,
- B denote the 120 degree clockwise rotation of the tip/middle layer containing the back corner.

Let $G =< R, L, U, B, r, l, u, b >$ denote the pyraminx group.

Each move $g \in G$ induces a permutation of E denoted $\sigma(g)$. Note that G does not permute the vertices. Furthermore, the tip moves r, l, u, b do not effect the edges.

Lemma 211. *$\sigma : G \to S_E$ is a group homomorphism.*

Example 212. $\rho(L)$ is a 3-cycle in S_V, $\sigma(L)$ is a 3-cycle in S_E.

11.3.1 Orientations

Assume for the moment that the pyraminx is fixed in space as above and is in the "solved" position. For each corner or edge piece, choose once and for all one facet on that piece. There are three possible choices for each corner piece and two for the edges. Mark each of these choosen facets with an imaginary '+', leaving the other facets unmarked. For the rest of this section, we shall make the following choices for the marked facets (with reference to the numbering in §4.7):

- marked edge facets: $4, 6, 10, 15, 20, 25$
- marked corner facets: $1, 13, 17, 23$

For each edge piece, assign to a move $g \in G$ either

- a '0' if the '+ facet' for that piece when it was in the solved position is sent to the '+ facet' for that piece when it was in the present position,
- a '1' otherwise,

This yields a 6-tuple of 0's and 1's: $\vec{w}(g) = (w_1, w_2, ..., w_6)$.

Example 213. We compute the effect of the basic twist moves on the edge orientations:

X	$\vec{w}(X)$
B	(0,0,0,1,0,1)
R	(0,0,1,0,1,0)
L	(1,0,1,0,0,0)
U	(0,1,0,1,0,0)
$R * U^{-1} * R^{-1} * U$	(1,1,0,0,0,0)

For each corner piece, assign to a move $g \in G$ either

- a '0' if the '+ facet' for that piece when it was in the solved position is sent to the '+ facet' for that piece in the present position,
- a '1' if the '+ facet' for that piece when it was in the solved position is sent to the facet which is a 120 degrees rotation about its vertex from the '+ facet' for that piece in the present position,
- a '2' otherwise, thus yielding a 4-tuple of 0's, 1's, and 2's: $\vec{v}(g) = (v_1, v_2, v_3, v_4)$.

Example 214. We compute the effect of the basic twist moves on the corner orientations:

X	$\vec{v}(X)$
B	(0,0,0,2)
R	(0,0,2,0)
L	(0,2,0,0)
U	(2,0,0,0)

Proposition 215. *If* $\vec{w}(g) = (w_1, w_2, ..., w_6)$ *corresponds to a move* $g \in G$ *then*

$$w_1 + w_2 + ... + w_6 \equiv 0 (\text{mod } 2).$$

Observation: There is no corresponding condition for the v_1, ..., v_4, since corner moves move them around freely.

proof: The proof uses the following lemma, but is otherwise essentially the same as the corresponding fact (Theorem 202 (c)) which we proved for the Rubik's cube. The modifications required for the proof are left to the student as an exercise to test their understanding of the argument. □

Lemma 216. *For $g, h \in G$, we have*

$$\vec{w}(g * h) = \sigma(g)^{-1}(\vec{w}(h)) + \vec{w}(g).$$

proof: The proof is essentially the same as the corresponding fact (Lemma 199) which we proved for the Rubik's cube. The modifications required for the proof are left to the reader as an exercise. □

Lemma 217. *For $g, h \in G$, we have*

$$\vec{v}(g * h) = \vec{v}(h) + \vec{v}(g).$$

Exercise 11.3.1. Prove this lemma.

Let H denote the enlarged pyraminx group generated by G and the "illegal edge moves" (that is, one may physically remove the edge pieces and reassemble the pyraminx. Illegal center or corner moves are not allowed in H. Let

$$H^* = \{(s, x, y) \mid r \in S_V, s \in S_E, x \in C_3^4, y \in C_2^6\}$$

and define $* : H^* \times H^* \to H^*$ by

$$(s, x, y) * (s', x', y') = (s * s', x + x', s'(y) + y').$$

Theorem 218.

- *H^* is, with this operation, a group.*
- *There is are isomorphisms*

$$H \cong H^* \cong C_3^4 \times (C_2^6 \; {>\!\!\lhd} \; S_E),$$

and hence between H and the direct product of the tip moves C_3^4 and the wreath product

$$C_3^4 \times (S_E \text{ wr } C_2).$$

- *The map $G \to H^*$ defined by*

$$g \longmapsto (\sigma(g), \vec{v}(g), \vec{w}(g)),$$

is a homomorphism.

11.3.2 Center pieces

Each corner piece has 3 center pieces neighboring it.

Facts:

- These center pieces, in the middle layer down from the corner and never be moved into any other corner's middle layer.
- The center pieces associated to a corner can never be moved into a middle layer associated to another corner.
- The center pieces associated to a corner can always be color-aligned with the colors of the corner piece by a corner twist move.

The third part says, in other words, that the center pieces can always be "solved" by a corner piece.

11.3.3 The group structure

Theorem 219. *G is isomorphic to*

$$\{(s, x, y) \in H^* \mid s \text{ even}, y_1 + y_2 + ... + y_6 \equiv 0 (\text{mod } 2)\}.$$

The idea to prove this is to show that

- $$A_E =< \sigma(R), \sigma(L), \sigma(U), \sigma(B) >$$
- $$\begin{array}{ccc} G & \rightarrow & A_E, \\ g & \longmapsto & \sigma(g), \end{array}$$

  is surjective,
- $G \rightarrow \{(w_1, ..., w_6) \in C_2^6 \mid w_1 + ... + w_6 \equiv 0 (\text{mod } 2)\}$, $g \longmapsto \vec{w}(g)$, is surjective (as a map of sets).

Here's the proof of the first point: We can label (as in §5.10) the edges $1, 2, ..., 6$ so that the edges on the front face are $1, 2, 3$, resp., where the fl edge is 1, the fr edge is 2, and the fd edge is 3 (here f, r, l, and d denote the front face, right face, left face, and down face, resp.). The move $[R, U^{-1}] = R * U^{-1} * R^{-1} * U$ is the counterclockwise cyclic permutation $(1, 3, 2)$ of the edges on the f face. (This move does not affect any corners but does flip some edges, a fact which we may ignore for now since we are only concerned with the permutations now.) In particular, $(1, 3, 2)$ may be written as a product of the generators in $\{\sigma(R), \sigma(L), \sigma(U), \sigma(B)\}$. Now pick any $i \in \{4, 5, 6\}$ and let $s \in G$ denote a move which sends edge i to edge 2 and does not move edge 1 or 3. The move $s * [R, U^{-1}] * s^{-1}$ is the 3-cycle $(1, 3, i)$. It does not affect any corners or other edges. By Lemma 160, these permutations generate $A_6 \cong A_E$. □

The second point follows immediately from the first point proven above.

Here's the proof of the last point: The move $g = [R, U^{-1}]$ has the following effect on the orientation: $w(g) = (1, 1, 0, 0, 0, 0)$. The group

$$\{(w_1, ..., w_6) \in C_2^6 \mid w_1 + ... + w_6 \equiv 0 (\text{mod } 2)\} \cong C_2^5$$

is a vector space over $\mathbb{F}_2$. The 5 vectors listed in the table for the values for w are all independent. It follows from this and the group law for G proves that the map $g \longmapsto \vec{w}(g)$ is surjective. □

The theorem 219 above is thus proven.

11.4 A uniform approach

This section shall follow [GT] in a uniform discussion of the pyraminx, the 3×3 Rubik's cube, and the megaminx. Other puzzle groups are analyzed in [GT] (see also [B], chapter 2, [NST], chapter 19).

Notation: Let

- G_p (resp., G_R, G_m) denote the permutation puzzle group generated by the basic moves of the pyraminx (resp., the Rubik's cube, megaminx),
- V_p (resp., V_R, V_m) denote the set of vertex pieces of the pyraminx (resp., the Rubik's cube, megaminx),
- E_p (resp., E_R, E_m) denote the set of edge pieces of the pyraminx (resp., the Rubik's cube, megaminx),

- F_p (resp., F_R, F_m) denote the set of facets of the movable pieces of the pyraminx (resp., the Rubik's cube, megaminx).

11.4.1 General remarks

Let G, V, E, F (resp.) denote either G_p, E_p, V_p, F_p (resp.), or G_R, E_R, V_R, F_R (resp.), or G_m, E_m, V_m, F_m (resp.).

Lemma 220. *G acts on the set V, (resp., E, F).*

If g is any move in G then, since g acts on the sets V, E, and F, we may regard g

- as an element of the symmetric group S_V of V,
- as an element of the symmetric group S_E of E, or
- as an element of the symmetric group S_F of F.

These groups S_V, S_E, and S_F are different, so to distinguish these three ways of regarding g, let us write

- g_V for the element of S_V corresponding to g,
- g_E for the element of S_E corresponding to g,
- g_F for the element of S_F corresponding to g.

What is the kernel of f_V? What is its image? To answer this question (actually, we shall not answer this precise question but one similar to it) we introduce a certain subgroup of the symmetric group.

Recall the alternating group A_X is the subgroup of all even permutations of X (in the sense of Example 82 above).

11.4.2 Parity conditions

Consider the function

$$\begin{aligned} f_{VE} : G &\to S_V \times S_E \\ g &\longmapsto (g_V, g_E) \end{aligned}$$

It is easy to check that this is a homomorphism.

Theorem 221. *The image $f_{VE}(G)$ of f_{VE} is isomorphic to*

$$\begin{cases} A_V \times A_E, & \text{for the pyraminx, megaminx,} \\ \{(x,y) \in S_V \times S_E \mid x, y \text{ both even or both odd}\}, & \text{for Rubik's cube.} \end{cases}$$

This is a consequence of a result proven below in the case of the Rubik's cube. To see what this theorem means, we look at an example.

Example 222. Let $G = G_R$.

Question: Can you find a move of the Rubik's cube which flips a single edge subcube over, leaving the rest of the puzzle pieces unmoved?

If so, then the image of f_{EV} would have to contain an element (x, y) with $x = 1$ (since moving an edge only does not effect the vertices) and where y is a 2-cycle. But $x = 1$ is even and a 2-cycle is odd. This contradicts the theorem, which says that x, y are either both even or both odd. Therefore, the answer is no: a single edge flip is impossible.

Next, some more **notation**: let

$$K = ker(f_{VE}) \lhd G$$

denote the kernel of the map f_{VE} introduced above. This is a normal subgroup of G.

Example 223. In the case of the Rubik's cube, this subgroup K is the set of moves which may reorient (i.e., flip or rotate) a subcube but does not swap it with some other subcube. For example, the move

$$(R^{-1} * D^2 * R * B^{-1} * U^2 * B)^2,$$

which twists the ufr corner clockwise and the bld corner counterclockwise, belongs to K.

Theorem 224. *(Gold, Turner [GT]) G is a semi-direct product of K with $f_{VE}(G)$.*

This is a consequence of a result proven above in the case of the Rubik's cube. In the case of the 3×3 Rubik's cube, some more details are given in chapter 10. See also [GT] or [NST], chapter 19.

Chapter 12

Interesting subgroups of the cube group

> "[Lefschetz and Einstein] had a running debate for many years. Lefschetz insisted that there was difficult mathematics. Einstein said that there was no difficult mathematics, only stupid mathematicians. I think that the history of mathematics is on the side of Einstein."
>
> *Richard Bellman*
>
> *EYE OF THE HURRICANE, 1984*

It is remarkable that several "familiar" groups may be embedding into the Rubik's cube group, and hence be regarded as a subgroup of the cube group. For example, we have seen in an earlier chapter how to embed the group of quaternions $Q = \{1, -1, i, -i, j, -j, k, -k\}$ inside the Rubik's cube group.

The subgroup method, discussed in the appendix, is a method for investigating God's algorithm using a computer. One of the groups arising in this method is the group studied in the first section of this chapter. The second section studies the "two faces" group.

12.1 The squares subgroup

Let G denote the subgroup of the Rubik's cube group generated by the *squares* of the basic moves:

$$G :=< U^2, D^2, R^2, L^2, F^2, B^2 >$$

called the squares group. We shall verify below that the order of this group is $2^{13}3^4$. (By the way, as a consequence of this and Burnside's theorem [R], ch. 5, it follows that G is a solvable group. We shall not need this fact.) In this section, we will investigate the group struction of G using the same method which was used to determine the structure of the Rubik's cube group.

The group G acts on the set of edges and the set of vertices of the cube. There is a choice of orientation of the edges (resp., corners) similar to that in §§10.1.2-3 such that each element of G *preserves the edge (resp., corner) orientations.*

The action ϕ of G on the edges E of the cube has exactly 3 orbits: the middle slice parallel to the right face E_R, the middle slice parallel to the front face E_F, the middle slice parallel to the up face E_U. In particular, the group G acts (by restriction) on E_R, E_F, and E_U. The action ψ of G on the set of vertices V has exactly 2 orbits: $V_1 = \{ufr, ubl, dfl, drb\}$, $V_2 = \{ufl, ubr, dfr, dlb\}$. Therfore, the group G acts (by restriction) on V_1 and V_2. These actions yield associated homomorphisms:

$$\begin{gathered}\phi : G \to S_E,\\ \phi_{E_R} : G \to S_{E_R},\\ \phi_{E_F} : G \to S_{E_F},\\ \phi_{E_U} : G \to S_{E_U},\\ \psi : G \to S_V,\\ \psi_1 : G \to S_{V_1},\\ \psi_2 : G \to S_{V_2}.\end{gathered}$$

Proposition 225. $G = \phi(G) \times \psi(G)$.

The proof of this is left as an exercise (hint: use the second fundamental theorem of Rubik's cube theory).

Lemma 226. *If $g \in G$ then*

$$sgn(\phi_{E_R}(g))sgn(\phi_{E_F}(g))sgn(\phi_{E_U}(g)) = 1.$$

Conversely, if $(p_1, p_2, p_3) \in S_{E_R} \times S_{E_F} \times S_{E_U}$ *then there is a* $g \in G$ *such that* $p_1 = \phi_{E_R}(g)$, $p_2 = \phi_{E_F}(g)$, $p_3 = \phi_{E_U}(g)$ *if and only if* $sgn(p_1)sgn(p_2)sgn(p_3) = 1$.

As a consequence, we find that

$$\phi(G) = ker(sgn \times sgn \times sgn : \phi_{E_R}(G) \times \phi_{E_F}(G) \times \phi_{E_U}(G) \to \{\pm 1\}) \cong (S_4 \times S_4 \times S_4)/C_2.$$

In particular, $|\phi(G)| = (4!)^3/2 = 2^8 3^3$.

It remains to determine $\psi(G)$. We denote this group by H for notational simplicity. We may label the vertices of the cube $1, 2, ..., 8$ in such a way that $H =< u, d, l, r, f, b >$, where $u = (1,3)(2,4), f = (1,8)(4,5), d = (5,7)(6,8), b = (3,6)(2,7), r = (2,5)(1,6), l = (4,7)(3,8)$. The action of H on the set of vertices of the cube has two orbits ($\{1,3,6,8\}$ and $\{2,4,5,7\}$ in our labeling above), which we denote for simplicity by V_1 and V_2. There are homomorphisms

$$\psi_1 : H \to S_{V_1}, \quad \psi_2 : H \to S_{V_2},$$

but we shall not say much about these. Instead, we use GAP [Gap] to determine more about H. According to GAP, this group has $|H| = 96$ elements and 10 conjugacy classes (by the way, GAP also says that all the generators $u, ..., b$ are conjugate):

size	representative
1	1
12	d=(5,7)(6,8)
32	l*d=(3,6,8)(4,5,7)
3	d*l*b*l=(2,4)(5,7)
12	d*b*l=(2,4,7,5)(3,6)
3	l*b*l*u=(1,3)(6,8)
12	b*l*u=(1,3,6,8)(4,7)
3	u*d=(1,3)(2,4)(5,7)(6,8)
12	l*d*u=(1,3,6,8)(2,4,5,7)
6	u*r*d*f=(1,3)(2,5)(4,7)(6,8)

The stabilizer in H of any vertex $v \in V$, written H_v, is a subgroup of order 24 isomorphic to the symmetric group S_4.

Furthermore, H has a normal subgroup N of order 48 (and index 2), where N is a semidirect product of C_3 by C_2^4, with C_2^4 normal in N.

This is all we shall say about H.

The order of G is therefore $G = |\phi(G)| \cdot |H| = 96 \cdot (4!)^3/2 = 2^{13}3^4$, as claimed above.

12.2 $PGL(2, \mathbb{F}_5)$ and two faces of the cube

The material in this section was communicated to me by Dan Bump (the idea originally arose in D. SIngmaster's [Si]). This section is relatively advanced in that it requires more mathematical background from the reader than the previous chapters.

This section is devoted to "determining" the two-face group generated by only two basic moves, $< F, U >$. D. Singmaster [Si] has shown that

$$< F, U > \cong S_7 \times PGL_2(\mathbb{F}_5),$$

where $PGL_2(\mathbb{F}_5)$ is a group of order 120 which is defined below. Here S_7 arises from the action of the Rubik's cube group on the edges and $PGL_2(\mathbb{F}_5)$ arises from the action on the corners. In this chapter, we focus on the action on the corners.

12.2.1 Finite fields

In this subsection, we introduce fields and especially finite fields.

The general definition

A field is a set F with an addition law $+$ and a multiplication law $\cdot$ which obeys the a list of properties similar to those for the field of real numbers $\mathbb{R}$. More precisely, we call $(F, +, \cdot)$ a field if

(F1) $(F, +)$ is an abelian group, with an identity element denoted 0 ("the additive group of the field"),

(F2) for all $x, y, z \in F$, $(x + y)z = xz + yz$ ("distributive law"),

(F3) $(F - \{0\}, \cdot)$ is an abelian group, with an identity element denoted 1 ("the multiplicative group of the field").

It happens to be true that if F is a finite field then not only is $(F - \{0\}, \cdot)$ an abelian group, it is actually a cyclic group.

Definition 227. Let F_1, F_2 be wo fields. A function $f : F_1 \to F_2$ is called a field isomorphism if

(a) when f is restricted to the additive group $(F_1, +)$, call this restriction f again, it yields an isomorphism of groups $f : (F_1, +) \to (F_2, +)$,

(b) when f is restricted to the multiplicative group $(F_1 - \{0\}, \cdot)$, call this restriction f again, it yields an isomorphism of groups $f : (F_1 - \{0\}, \cdot) \to (F_2 - \{0\}, \cdot)$.

A construction of $\mathbb{F}_p$

Recall from §2.3 that congruence modulo n ($n > 1$ an integer) is an equivalence relation. Let $n = p$ be a prime and let $\overline{k}$ denote the equivalence class of k with respect to this equivalence relation. Let $\mathbb{F}_p$ denote the finite field with p elements, so $\mathbb{F}_p$ is, as a set,

$$\mathbb{F}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\},$$

with addition and multiplication being performed mod p.

Example 228. When $p = 5$, $\mathbb{F}_5$ will denote the finite field with 5 elements, so $\mathbb{F}_5$ is, as a set,

$$\mathbb{F}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\},$$

with addition and multiplication being performed mod 5.

It is a general fact that if F is any finite field then there is a prime number p such that $px = 0$ for all $x \in F$. This prime number is called the characteristic of F. The easiest example of a finite field with characteristic p is the finite field having p elements, $\mathbb{F}_p$. It is not hard to see that any other finite field F of characteristic p must be a finite dimensional vector space over $\mathbb{F}_p$. (Even if you've never seen a "vector space over $\mathbb{F}_p$" defined before, if you know what a "real vector space" is then you've got the right idea.) The dimension of the vector space F is called the degree of F over $\mathbb{F}_p$, denoted $d = [F : \mathbb{F}_p]$, and F is called a field extension of $\mathbb{F}_p$ of degree d. It is a general fact that for fixed p, d there is, up to isomorphism, only one such field.

Next, we shall show how to construct in a very simple way such extensions.

A construction of finite fields

First, some general remarks. Since F is a finite dimensional vector space containing $\mathbb{F}_p$, it has a vector space basis which we label as

$$e_1 = 1, e_2, ..., e_d.$$

Thus F is, as a set, the collection of elements of the form

$$x_1 e_1 + ...x_n e_n, \qquad x_i \in \mathbb{F}_p.$$

Since F is a field, there are $c_{ij}^k \in \mathbb{F}_p$, which we call structure constants, such that

$$e_i e_j = \sum_{k=1}^{n} c_{ij}^k e_k.$$

There are $d_i^k \in \mathbb{F}_p$, which we call inversion constants, such that

$$e_i^{-1} = \sum_{k=1}^{n} c_i^k e_k.$$

These constants determine how to multiply and divide elements of F. We shall consider F "completely described" once we explicitly determine these constants.

Example 229. Let $p = 5$, so $\mathbb{F}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. The set of squares is given by

$$\{x^2 \mid x \in \mathbb{F}_5\} = \{\overline{0}, \overline{1}, \overline{4}\}.$$

In particular, $\overline{2}, \overline{3}$ are not squares in this field. Let $e_2 = \sqrt{\overline{2}}$ be a formal symbol for some element which satisfies $e_2^2 = \overline{2}$. This is a root of the polynomial $x^2 - \overline{2} = 0$.

The vector space F over $\mathbb{F}_5$ with basis $\{e_1 = 1, e_2\}$ is 2-dimensional over $\mathbb{F}_5$. Two elements $x_1 e_1 + x_2 e_2 = x_1 + x_2\sqrt{\overline{2}}$ and $y_1 e_1 + y_2 e_2 = y_1 + y_2\sqrt{\overline{2}}$ are multiplied by the rule

$$(x_1 + x_2\sqrt{\overline{2}}) \cdot (y_1 + y_2\sqrt{\overline{2}}) = x_1 y_1 + \overline{2} x_2 y_2 + (x_1 y_2 + y_1 x_2)\sqrt{\overline{2}}.$$

It is a degree 2 field extension since

$$c_{11}^1 = \overline{1}, \quad c_{11}^2 = \overline{0}, \quad c_{12}^1 = \overline{0}, \quad c_{12}^2 = \overline{1}, \quad c_{21}^1 = \overline{2}, \quad c_{21}^2 = \overline{0},$$

and

$$d_1^1 = \overline{1}, \quad d_1^2 = \overline{0}, \quad d_2^1 = \overline{0}, \quad d_2^2 = \overline{3}.$$

The construction used in the above example may be summarized more generally as follows:

1. Pick an element $m \in \mathbb{F}_p$ which is not the square of another element.
2. Let $e_1 = 1$ and $e_2 = \sqrt{\overline{m}}$ be a formal symbol for some element which satisfies $e_2^2 = \overline{m}$.
3. As a set, let $F = \{xe_1 + ye_2 \mid x, y \in \mathbb{F}_p\}$. To define F as a field, let $+$ be "componentwise addition" mod p and let $\cdot$ be defined by

$$(x_1 + x_2\sqrt{\overline{m}}) \cdot (y_1 + y_2\sqrt{\overline{m}}) = x_1y_1 + \overline{m}x_2y_2 + (x_1y_2 + y_1x_2)\sqrt{\overline{m}}.$$

A finite field F constructed in this way is called a quadratic extension of $\mathbb{F}_p$.

More generally, let $d > 1$ be an integer.

1. Pick an element $m \in \mathbb{F}_p$ which is not the d^{th} power of another element.
2. Let $e_1 = 1$, let $e_2 = \overline{m}^{1/d}$ be a formal symbol for some element which satisfies $e_2^d = \overline{m}$, and (if $d > 2$) let $e_i = e_2^{i-2}$ for $i = 3, ..., d$.
3. As a set, let $F = \{x_1e_1 + ... + x_de_d \mid x_i \in \mathbb{F}_p\}$. To define F as a field, let $+$ be "componentwise addition" mod p and let $\cdot$ be defined by expanding and collecting $(x_1e_1 + ... + x_de_d) \cdot (y_1e_1 + ... + y_de_d)$.

A finite field F constructed in this way is called a degree d extension of $\mathbb{F}_p$. It has p^d elements. It turns out that any two fields having p^d elements must be isomorphic. Therefore, any finite field must be isomorphic to one described above.

Definition 230. The projective plane

$$\mathbb{P}^1(\mathbb{F}_p) = \{\overline{0}, \overline{1}, ..., \overline{p-1}, \infty\}$$

is defined to be the set of lines through the origin in the Cartesian plane $\mathbb{F}_p^2$, associating each number (including ∞) with the slope of the corresponding line.

12.2.2 Möbius transformations

If $a, b, c, d \in \mathbb{F}_p$ are given numbers (not all equal to zero) then we define the Mobius transformation f by:

$$\begin{array}{c} f : \mathbb{P}^1(\mathbb{F}_p) \to \mathbb{P}^1(\mathbb{F}_p) \\ x \longmapsto \frac{ax+b}{cx+d}. \end{array}$$

Theorem 231. *f is a bijection if and only if* $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0.$

Before proving this, we need the following

Definition 232. Define

$$GL(2, \mathbb{F}_5) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_5, \ ad - bc \neq 0 \}.$$

This set is a group under ordinary matrix multiplication and, furthermore, acts on the set $\mathbb{P}^1(\mathbb{F}_5)$ by means of Mobius transformations thus defining a function

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathbb{P}^1(\mathbb{F}_5) \to \mathbb{P}^1(\mathbb{F}_5)$$

Lemma 233. *(a) The center of $GL(2, \mathbb{F}_p)$ (i.e., the subgroup of all elements which commute with every element in $GL(2, \mathbb{F}_p)$) is given by*

$$Z(GL(2, \mathbb{F}_p)) = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p, \ a \neq 0 \}.$$

(b) This subgroup is normal in $GL(2, \mathbb{F}_p)$.
(c) There is an isomorphism

$$Z(GL(2, \mathbb{F}_p)) \cong \mathbb{F}_p^{\times}.$$

proof: (a) Since

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we can conclude that

$$\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p, \ a \neq 0 \} \subset Z(GL(2, \mathbb{F}_p)).$$

To show that

$$Z(GL(2,\mathbb{F}_p)) \subset \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p,\ a \neq 0\},$$

assume that

$$\begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for all a, b, c, d. This implies $bu = cs$ for all b, c. This is impossible unless $u = s = 0$. This in turn forces $cr = cv$, for all c. This implies $r = v$. This proves the desired inclusion.

The proof of parts (b) and (c) are left as an exercise for the reader. □

Definition 234. The quotient group, denoted $PGL(2,\mathbb{F}_p) = GL(2,\mathbb{F}_p)/Z(GL(2,\mathbb{F}_p))$, is called the projective linear group. (This is a group since the center is a normal subgroup by the lemma above.)

Lemma 235. *This group $PGL(2,\mathbb{F}_p)$ acts on the set $\mathbb{P}^1(\mathbb{F}_p)$ by means of the linear fractional transformations.*

Remark 24. In fact, the action of $PGL(2,\mathbb{F}_p)$ on the set $\mathbb{P}^1(\mathbb{F}_p)$ is 3-transitive. This not hard to prove but we left it to the interested reader to look it up in [R] (see Theorem 9.48).

proof: First, we show that the $GL(2,\mathbb{F}_p)$ acts on the set $\mathbb{P}^1(\mathbb{F}_p)$ by means of the linear fractional transformations. In other words, if

$$\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x) = \frac{ax+b}{cx+d}$$

then

(a) $\phi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(x) = x$, for all x (i.e., the linear fractional transformation $\phi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity map),

(b) $\phi(A) \circ \phi(B) = \phi(AB)$, for all $A, B \in GL(2,\mathbb{F}_p)$.

We leave (a) to the reader and check (b). Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$. Then

$$AB = \begin{pmatrix} ar+bu & as+bv \\ cr+du & cs+dv \end{pmatrix},$$

so

$$\phi(AB)(x) = \frac{(ar+bu)x + as + bv}{(cr+du)x + cs + dv}.$$

On the other hand, $\phi(A)(\phi(B)(x))$ is equal to

$$\phi(A)(\frac{rx+s}{ux+v}) = \frac{a(\frac{rx+s}{ux+v}) + b}{c(\frac{rx+s}{ux+v}) + d}.$$

Simplifying this, we see that the last two displayed equations are equal. This verifies (b).

Therefore, $GL(2, \mathbb{F}_p)$ acts on the set $\mathbb{P}^1(\mathbb{F}_p)$.

Let $Z = Z(GL(2, \mathbb{F}_p))$. Since $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \phi \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix}$, for all non-zero r, it follows that we may define an action of $PGL(2, \mathbb{F}_p)$ on the set $\mathbb{P}^1(\mathbb{F}_p)$ by $\phi(A \cdot Z) = \phi(A)$, for all $A \in GL(2, \mathbb{F}_p)$.

□

proof of the theorem: Let ϕ be as above and let f be as in the statement of the theorem.

($\Leftarrow$): Since $GL(2, \mathbb{F}_p)$ acts on the set $\mathbb{P}^1(\mathbb{F}_p)$, we have $1 = \phi(AA^{-1}) = \phi(A)\phi(A^{-1})$, so $\phi(A)$ is invertible. This implies that f is a bijection.

($\Rightarrow$): We prove the contrapositive. Suppose that $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0$. By a result in linear algebra (see any text book, for example [JN]), the row vectors of this matrix are linearly dependent. This implies that there is an $r \in \mathbb{F}_p$ such that either $(a, b) = r \cdot (c, d)$ or $(c, d) = r \cdot (a, b)$. In either case, the quotient $f(x) = \frac{ax+b}{cx+d}$ is a constant independent of x, so cannot be surjective. This proves that f is not a bijection, which verifies the contrapositive.

□

12.2.3 The main isomorphism

Let G denote the Rubik's cube group. Let H be the subgroup generated by F and U:

$$H =< F, U > .$$

Exercise 12.2.1. Show the group H acts on the set of vertices above (via the Rubik's cube group).

We describe how to label the six vertices on the "up" and "front" faces of the cube,

$$fru, flu, dfl, dfr, bru, blu,$$

with the elements in the projective plane

$$\mathbb{P}^1(\mathbb{F}_5) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \infty\}$$

in a certain way. More precisely, we will show label the 6 vertices above with elements of $\mathbb{P}^1(\mathbb{F}_5)$ in such a way that (a), (b) of the following theorem hold true.

Theorem 236. *There are $a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 \in \mathbb{F}_5$ (given explicitly below) such that*

(a) the action of F (the usual rotation of the front face) on these vertices is the same as the action of some linear fractional transformation

$$f_F(x) = \frac{a_0 x + b_0}{c_0 x + d_0}$$

(b) the action of U (the usual rotation of the up face) on these vertices is the same as the action of some linear fractional transformation

$$f_U(x) = \frac{a_1 x + b_1}{c_1 x + d_1}$$

In other words, the basic moves F, U may be regarded as linear fractions transformations over a finite field!

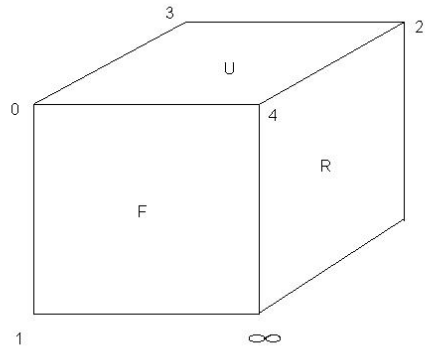
Theorem 237. $PGL(2, \mathbb{F}_5) =< f_F, f_U >$.

Remark 25. $PGL(2, \mathbb{F}_5)$ is isomorphic to S_5 (this is part of Exercise 9.25 in [R]).

We shall prove these below.

12.2.4 The labeling

Label the up and front vertices as



Let

$$f_F(x) = \frac{x-1}{x+1}, \qquad f_U(x) = 3x+3.$$

The map

$$\phi : F \longmapsto f_F, \quad U \longmapsto F_U,$$

extends to a surjective homomorphism of groups

$$\phi \ : < F, U > \ \rightarrow \ < f_F, f_U > \subset \ PGL(2, \mathbb{F}_5).$$

Exercise 12.2.2. Verify the first theorem above.

12.2.5 Proof of the second theorem

Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}_* \in PGL(2, \mathbb{F}_F)$$

denote the image of

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{F}_F)$$

under the natural map $GL(2, \mathbb{F}_5) \rightarrow PGL(2, \mathbb{F}_5)$, $g \longmapsto \mathbb{F}_5^\times * g$.

Since

$$f_U^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_*$$

we have

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_* \in < f_U, f_F > .$$

Since

$$f_F * f_U^5 = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}_*$$

it follows that

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}_* \in < f_F, f_U > .$$

Conjugating this matrix by f_U^2, we find that

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}_* \in < f_F, f_U > .$$

It is known that $SL(2, \mathbb{F}_5)$ is generated by elementary transvections (see [R]). Therefore,

$$PSL(2, \mathbb{F}_5) \subset < f_F, f_U > \subset PGL(2, \mathbb{F}_5).$$

It is also known (see [R]) that

$$|PSL(2, \mathbb{F}_5)| = 60 \quad \text{and} \quad |PGL(2, \mathbb{F}_5)| = 120.$$

It remains to show that there is an element of $< f_F, f_U >$ which does not belong to $PSL(2, \mathbb{F}_5)$. We claim that such an element is f_U. Note that $\det(f_U)$ belongs to the set

$$3(\mathbb{F}_5^\times)^2 = \{3x^2 \mid x \in \mathbb{F}_5^\times\}.$$

But an element of $PSL(2, \mathbb{F}_5)$ must have determinant 1. Since $3^{-1} = 2 \pmod 5$ is not a square mod 5, there is no element of $\mathbb{F}_5$ which satisfies $1 = 3x^2$. Thus f_U does not belong to $PSL(2, \mathbb{F}_5)$. □

Exercise 12.2.3. As an application of theorem 237, use the example in section 5.4.2 to show that there exists an embedding $D_{12} \hookrightarrow PGL(2, \mathbb{F}_5)$ of the symmetry group of the hexagon into $PGL(2, \mathbb{F}_5)$.

12.3 The cross groups

Define a cross move of the cube to be a move of the form $X * Y^{-1}$, where $X, Y \in \{R, L, U, D, F, B\}$. The subgroup of the Rubik's cube group generated by the cross moves will be called the cross group.

The cross moves permute the set V of vertices of the cube and therefore generate a subgroup of S_V. This is called the vertex cross group. The cross moves permute the set E of edges of the cube and therefore generate a subgroup of S_E. This is called the edge cross group.

All the enties in the following table are, as far as I am aware, are new except for the M_{12} entry.

Rubik polyhedra	edge cross group	vertex cross group
tetrahedron	$A_5 \cong PSL_2(\mathbb{F}_5)$	$C_2 \times C_2$
cube	A_{12}	$PSL_2(\mathbb{F}_7)$
octahedron	A_{12}	$PSL_2(\mathbb{F}_5)$
dodecahedron	A_{30}	A_{20}
icosahedron	A_{30}	A_{12}
rubicon	A_{30}	M_{12}

In fact, the subgroup of the dodecahedral edge cross group generated by a subset of the cross moves can yield (smaller but still simple) alternating groups.

Problem: (F. Dyson) Work out the analogous cross groups of the "Rubicized" 4-dimensional regular polyhedra.

This is only known for the 4-dimensional Rubik's hypercube. In the 4-dimensional case, one can also define the face cross group since the moves of the 4-dimensional Rubik's hypercube also permute the set F of 2-dimensional faces. We have the following results:

Rubik polyhedra	edge cross group	vertex cross group	face cross group
4-dimensional cube	A_E	A_V	A_F

Problem: Are any of the analogous cross groups of the "Rubicized" 3-dimensional Archimedian polyhedra simple?

It appears that the vertex cross group of the regular truncated cube is not simple.

12.3.1 $PSL(2, \mathbb{F}_7)$ and crossing the cube

Let C denote the vertex cross group of the Rubik's cube.

Theorem 238. $C \cong PSL_2(\mathbb{F}_7)$.

The first proof of this is by computer!

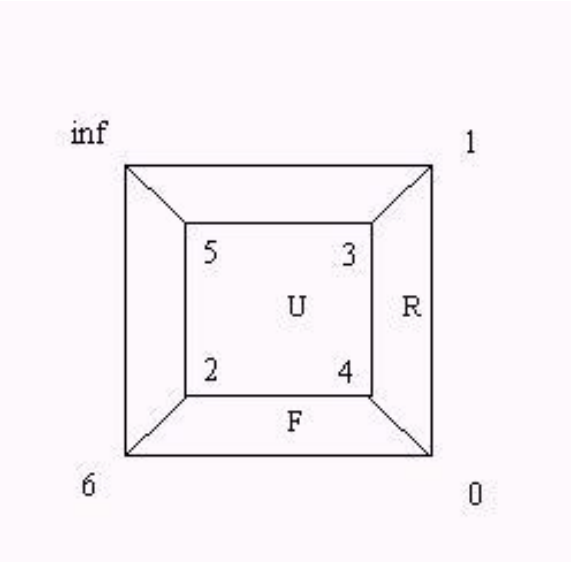
first proof: Gap [Gap] gives that C is a simple group of order 168. By the classification of simple groups (or, more simply, Exercise 9.26 in [R]), C must be isomorphic to $PSL_2(\mathbb{F}_7)$. $\square$

The second proof is from [CD].

second proof: $PSL_2(\mathbb{F}_7)$ can be generated by the three matrices:

$$f_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, f_2 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

We will label the vertices of the cube in the following manner:



Labeling the cube by the projective line $P^1(\mathbb{F}_7)$

Under this labeling, we can show that

- the image of the move $m_1 = (UD^{-1})^2$ will permute the vertices in this way: $(\infty, 0)(1, 6)(2, 3)(4, 5)$, The same permutation is given by the mobius transform $(0x - 1)/(x + 0)$ acting on $P^1(\mathbb{F}_7)$.
- $m_2 = UR^{-1}$ gives us the permutation: $(0, 1, 3)(2, 5, 4)$, which is given by $(2x + 1)/(0x + 1)$ acting of $P^1(\mathbb{F}_7)$.
- $m_3 = BU^{-1}LB^{-1}$ gives us the permutation $(1, 2, 4)(3, 6, 5)$, which is given by $(2x + 0)/(0x + 1)$ acting on $P^1(\mathbb{F}_7)$.

You should notice that if the constants in these Möbius transformations (a, b, c, d) are written in matrix form, they correspond to the generators of $PSL_2(\mathbb{F}_7)$. Now we will define a homomorphism $q : C \to PSL_2(\mathbb{F}_7)$, such that $q(m_1) = f_1, q(m_2) = f_2, q(m_3) = f_3$. We want to show that our q is an isomorphism.

To do this we will first show that it is surjective. Let f be a matrix in $PSL_2(\mathbb{F}_7)$, which can be written as a product of generators f_1, f_2, f_3 (where $q(m_1) = f_1, q(m_2) = f_2, q(m_3) = f_3$). Now take f as some element of $PSL_2(\mathbb{F}_7)$. f can be broken down as a product of its generators, f_1, f_2, f_3, we'll say

$$f = \prod_{k=1}^{n} f_{i_k}^{e_k}.$$

Since we have a homomorphism, we can write it as a product of the images of the generators of C. Again we can rewrite it as $f = q(\prod_{k=1}^{n} m_{i_k}^{e_k})$. Therefore q is surjective.

To show that q is one to one we need to know that $PSL_2(\mathbb{F}_7)$ has order 168 [R], and that the order of the cross group is also 168. (This fact was proven by computer.) We will prove by contradiction that q is one to one.

Now we assume that c_1 and c_2 are elements of C, such that $q(c_1) = q(c_2)$, and c_1 is not equal to c_2. $|PSL_2(\mathbb{F}_7)| = |q(C)|$. We now subtract c_2 from C , and $|q(C)| = |q(C - c_2)|$ because $q(c_1) = q(c_2)$. Now we can say that $|q(C - c_2)| < or = |C - c_2|$ because we know that q is surjective.

Since we have taken c_2 out of C, we know $|C - c_2| < |C|$, which by transitivity implies $|PSL_2(\mathbb{F}_7)| < |C|$. This is a contradiction because we know $|PSL_2(\mathbb{F}_7)| = |C|$. Therefore q is injective.

Now that we have shown that q is both surjective and injective, it is bijective and an isomorphism. □

The above proof of the theorem tells us explicitly that there exists a labeling of the vertices V of the cube by the elements of the projective line

$$\mathbb{P}^1(\mathbb{F}) = \{\infty, \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\},$$

with the property that there is a move $c : V \to V$ in C if and only if there is a Möbius transformation $f : \mathbb{P}^1(\mathbb{F}) \to \mathbb{P}^1(\mathbb{F})$ in $PSL_2(\mathbb{F}_7)$.

Because the group of Möbius transformations in $PSL_2(\mathbb{F}_7)$ acts 2-transitively on the projective line $\mathbb{P}^1(\mathbb{F})$ (see [R], Theorem 9.45), it follows that we have the following

Corollary 239. *C acts 2-transitively on V. In other words, for any ordered pairs (v_1, v_2), (v_1', v_2) of distinct vertices there is an element $c \in C$ sending v_i to v_i', for $i = 1, 2$.*

12.3.2 Klein's 4-group and crossing the pyraminx

We leave the main result of this section as an Exercise - actually more of a project - for the reader.

Exercise 12.3.1. (hard) Show that the subgroup of S_V generated by the twist-untwist moves of the pyraminx is isomorphic to the Klein 4 group $C_2 \times C_2$.

The determination of the cross group for the megaminx is due to J. Conway. It will be presented in the next chapter.

Chapter 13

Crossing the Rubicon

"Mathematical structures are among the most beautiful discoveries by the human mind. The best of these discoveries have tremendous metaphorical and explanatory power."

Douglas Hofstadter
METAMATHEMATICAL THEMAS, 1985

Much of the material here can be found in [CS] and is due to John Conway. The title of this chapter is, however, "borrowed" from a similarly worded title of an article by D. Hofstadter [H]. More details on parts of this chapter may be found in Ann Luers' paper [Lu].

This chapter shall be a little more advanced than some of the others. The reader will be assumed to be familiar with some topics covered in a course in linear algebra and elementary number theory or coding theory. We shall also assume some results from Rotman [R], though for the understanding of the material in this chapter the reader may simply take them on faith.

Let $g_1, ..., g_{12}$ denote the basic moves of the Rubik isocahedron. A surprising result of Conway states that the group generated by $g_i * g_j^{-1}$ is the simple "sporadic" group M_{12}. (This is stated more precisely below.) We shall describe, in this chapter, what M_{12} is and some of its remarkable properties. They form a basis for my opinion, which I hope you will agree with, that M_{12} is one of the most interesting objects in mathematics.

Let p be a prime unless otherwise stated and let q be a power of p. **We shall assume that $p > 3$.**

13.1 Doing the Mongean shuffle

Consider a deck of 12 cards labeled 0, 1, ..., 11. Let r, s be the permutations

$$r(t) = 11 - t, \qquad s(t) = min(2t, 23 - 2t).$$

The permutation r reverses the cards around and the permutation s is called the "Mongean shuffle". To perform the reverse shuffle, simply take a stack of cards (face down, say) in your left hand and put them in your right hand one-at-a-time (face down). To perform the Mongean shuffle, take the same stack of cards and, one-at-a-time, put them alternately into one of two piles: the first card face up into the first pile, the second card face down into the second pile, the third card face up into the first pile, the fourth card face down into the second pile, and so on until the pile is exhausted. Now pick up the first pile of face up cards, flip the entire pile over so that they are all fade down and put it on top of the second pile.

cards	reverse shuffle	Mongean shuffle
0	11	0
1	10	2
2	9	4
3	8	6
4	7	8
5	6	10
6	5	11
7	4	9
8	3	7
9	2	5
10	1	3
11	0	1

Definition 240. The Mathieu group M_{12} is defined to be the permutation group $M_{12} =< r, s > < S_{12}$.

13.2 Background on PSL_2

We need a few basic facts about the projective special linear group of degree 2. We have already discussed the related group $GL(2, \mathbb{F}_p)$ in the previous chapter, so we refer to there for more details.

Definition 241. (1^{st} version) Define $SL_2(\mathbb{F}_q)$ to be the group of all 2×2 matrices having entries taken from the finite field $\mathbb{F}_q$ and having determinant one. This is called the special linear group of degree 2 over $\mathbb{F}_q$. The center of this group, denoted Z, is the subgroup of 2×2 "scalar" matrices of the form $diag(z, z)$, where $z \in \{1, -1\}$. (This is a normal subgroup of $SL_2(\mathbb{F}_q)$.) Define $PSL_2(\mathbb{F}_q)$ to be the quotient $SL_2(\mathbb{F}_q)/Z$. This is called the projective special linear group of degree 2 over $\mathbb{F}_q$.

Definition 242. (2^{nd} version) Define the projective line $\mathbb{P}^1(\mathbb{F}_q)$ of the finite field $\mathbb{F}_q$ to be the $q+1$ values of the formal ratio x/y, where x, y run over all elements of $\mathbb{F}_q$. If $y = 0$ then we denote this formal value by ∞, so

$$\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}.$$

If $q = p$ is a prime then we denote

$$\mathbb{P}^1(\mathbb{F}_p) = \{\infty, 0, 1, ..., p-1\}.$$

Define $PSL_2(\mathbb{F}_q)$ to be the group of all Mobius transformations on the projective line

$$f(x) = (ax + b)/(cx + d), \qquad x \in \mathbb{P}^1(\mathbb{F}_q),$$

where $ad - bc = 1$ and $a, b, c, d \in \mathbb{F}_q$ (We define $f(\infty) = a/c$.)

Mobius transformations are bijections from the projective line to itself, so we may interpret each Mobius transformation as an element of S_X , where $X = \mathbb{P}^1(\mathbb{F}_q)$ (and therefore also of S_n, where $n = |\mathbb{P}^1(\mathbb{F}_q)| = q + 1$).

Example 243. Let $p = 11$ and let $f(x) = -1/x$. Then

x	$f(x)$
∞	0
0	∞
1	10
2	5
3	7
4	8
5	2
6	9
7	3
8	4
9	6
10	1

Therefore, as a permutation, $f = (\infty, 0)(1, 10)(2, 5)(3, 7)(4, 8)(6, 9)$.

The following facts are known about the projective special linear group:

Theorem 244. *If $q > 3$ then $PSL_2(\mathbb{F}_q)$ is a simple group. Moreover, for all prime powers q,*

$$|PSL_2(\mathbb{F}_q)| = (q^2 - 1)q/gcd(2, q - 1).$$

(Recall a simple group was defined in Definition 163.) This theorem is over 100 years old. It is proven, for example, in [R].

Theorem 245. *Choose a $k \in \mathbb{F}_q$ such that $< k >= \mathbb{F}_q^\times$. Let*

$$f_1(x) = x + 1, \quad f_2(x) = k \cdot x, \quad f_3(x) = -1/x.$$

Then $PSL_2(\mathbb{F}_q)$ is generated by f_1, f_2, and f_3. In particular, the action of $PSL_2(\mathbb{F}_q)$ on the projective line $X = \mathbb{P}^1(\mathbb{F}_q)$ yields an injective homomorphism $PSL_2(\mathbb{F}_q) \to S_X$.

Basically, this is proven in [R] as well.

13.3 Galois' last dream

Supposedly, the night before he died in a duel, Galois wrote a letter to a friend stating the following remarkable theorem:

Theorem 246. *(Galois) Assume $p > 11$. Then $PSL_2(\mathbb{F}_p)$ has no embedding into a symmetric group S_n with $n \leq p$.*

The following isomorphisms (for $q \leq 11$) are known:

$$PSL_2(\mathbb{F}_q) \cong \begin{cases} A_4, & q = 3, \\ A_5, & q = 5, \\ A_6, & q = 9. \end{cases}$$

If $p = 7$ or $p = 11$ then explicit embeddings of $PSL_2(\mathbb{F}_p)$ into A_8 ($p = 7$), A_{12} ($p = 11$) are known (see [CS], ch 10, or [K] for an excellent discussion of this).

13.4 The M_{12} generation

One of the most amazing aspects about M_{12} is its close relationship with other "interesting" groups.

Definition 247. Define the permutation f_4 of the set $\mathbb{P}^1(\mathbb{F}_p) = \{\infty, 0, 1, ..., p-1\}$, for $3 \leq p \leq 11$, as follows

$$f_4 = \begin{cases} 1, & p = 3, \\ (1,2)(3,4), & p = 5, \\ (1,2)(3,6), & p = 7, \\ (2,10)(3,4)(5,9)(6,7), & p = 11. \end{cases}$$

We have run across the group S_6 before, when studying the symmetries of the icosahedron. We have also seen that S_6 is rather an interesting group because it is the only non-abelian symmetric group S_n which has an outer automorphism. One rather connection between M_{12} and S_6 is given by the following

Theorem 248. *(a) If $p = 5$ then $S_6 =< f_1, f_2, f_3, f_4 >$.*
(b) If $p = 11$ then $M_{12} =< f_1, f_2, f_3, f_4 >$.

We shall see another interpretation of M_{12} below using coding theory!

Definition 249. Let

$$\delta(x) = \begin{cases} x^3/9, & x \in (\mathbb{F}_{23})^2 - 0, \\ 9x^3, & x \in \mathbb{P}^1(\mathbb{F}_{23}) - (\mathbb{F}_{23})^2. \end{cases}$$

This is an element of S_X, where $X = \mathbb{P}^1(\mathbb{F}_{23})$. Define the Mathieu group M_{24} by

$$< f, \delta \mid f \in PSL_2(\mathbb{F}_{23}) > .$$

This is a permutation group in S_X, where $X = \mathbb{P}^1(\mathbb{F}_{23})$.

By the way,
(a) $(\mathbb{F}_{23})^2 = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$,
(b) $M_{12} = 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 95040$,
(c) $|M_{24}| = 244823040$.

13.5 Coding the Golay way

Codes are used in everyday life, from ISBN numbers on books to barcodes on food products to music CDs to satellite transmissions. There are many types of codes, some more efficient than others, some with better error correcting ability than others, some more practical than others, and so on. We shall concern ourselves only with aspects which are related to (in one way or another) permutation puzzles.

Definition 250. A q-ary code is a subset C of a finite dimensional vector space V over the finite field $\mathbb{F}_q$. A code word is an element of C. The number of coordinates (i.e., the dimension of V) is called the length of the code word. If $q = 2$ then the code is called binary (instead of 2-ary) and if $q = 3$ then the code is called ternary (instead of 3-ary).

Example 251. $V = \mathbb{F}_q^n = \mathbb{F}_q \times ... \times \mathbb{F}_q$ (n times) is a code.

Definition 252. Let $Mon_n(\mathbb{F}_q)$ denote the group of all $n \times n$ matrices which have exactly one non-zero entry from $\mathbb{F}_q$ per row and per column. An element of $Mon_n(\mathbb{F}_q)$ is called a monomial matrix.

Exercise 13.5.1. (a) Show $Mon_n(\mathbb{F}_q)$ is a group.
(b) Show $|Mon_n(\mathbb{F}_q)| = (q-1)^n \cdot n!$.

Definition 253. The set of all $A \in Mon_n(\mathbb{F}_q)$ such that $A * C = C$ (i.e., are the same code) is called the automorphism group of C, denoted $Aut(C)$.

We shall see some examples below.

Definition 254. If w is a code word in $\mathbb{F}_q^n$ then number of non-zero coordinates of w is called the weight of w, denoted $wt(w)$.

A cyclic code is a code which has the property that whenever $(c_0, c_1, ..., c_{n-1})$ is a code word then so is $(c_{n-1}, c_0, ..., c_{n-2})$. If $(c_0, c_1, ..., c_{n-1})$ is a code word in a cyclic code V then we call

$$g(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

a generator polynomial for C .

Example 255. The code with elements

$$(1,1,0,1,0,0,0),(0,1,1,0,1,0,0),(0,0,1,1,0,1,0),(0,0,0,1,1,0,1)$$

is a binary cyclic code of length 7 and weight 3. It has generator polynomial

$$g(x) = 1 + x + x^3.$$

(This code is called a "Hamming code" and has many interesting properties which, to describe, would take us too far afield. The interested reader is refered to [CS], ch. 3.)

Definition 256. Let n be a positive integer relatively prime to q and let alpha be a primitive n-th root of unity. Each generator polynomial g of a cyclic code C of length n has a factorization of the form

$$g(x) = (x - \alpha^{k_1})...(x - \alpha^{k_r}),$$

where $\{k_1, ..., k_r\} \subset \{0, ..., n-1\}$. The numbers α^{k_i}, $1 \leq i \leq r$, are called the zeros of the code C. They do not depend on the choice of g.

Definition 257. Let p and n be distinct primes and assume that p is a square mod n. The quadratic residue code of length n over $\mathbb{F}_p$ is the cyclic code whose generator polynomial has zeros

$$\{\alpha^k \mid k \text{ is a square mod } n\}.$$

The binary Golay code GC_{23} is the quadratic residue code of length 23 over $\mathbb{F}_2$. The binary Golay code GC_{24} is the code of length 24 over $\mathbb{F}_2$ obtained by appending onto GC_{23} a zero-sum check digit.

The ternary Golay code GC_{11} is the quadratic residue code of length 11 over $\mathbb{F}_3$. The ternary Golay code GC_{12} is the code of length 12 over $\mathbb{F}_3$ obtained by appending onto GC_{11} a zero-sum check digit.

The following result illustrate how the Matheiu groups arise in coding theory.

Theorem 258. *(a) There is a normal subgroup N of $Aut(GC_{12})$ of order 2 such that $Aut(GC_{12})/N$ is isomorphic to M_{12}.*

(b) $Aut(GC_{24}) = M_{24}$.

Since the Mathieu groups are so large, this theorem above indicates that the Golay codes GC_{12} and GC_{24} have a lot of symmetry.

It is a basic rule of thumb in mathematics that whenever you find something displaying a lot of symmetry then it will quite often have other interesting properties. With this philosophy spurring us on, let us turn to some of the other properties of these codes.

Lemma 259. *Any two code words in GC_{24} differ by 8 bits. The code GC_{24} detects 4 errors (per 24 bits) and corrects 3 errors.*

When you compare that with the correcting ability of bar-codes or ISBN codes (which have a check-digit), GC_{24} is much better.

Lemma 260. *If w is a code word in GC_{24} then $wt(w)$ is either $0, 8, 12, 16, 24$.*

Definition 261. The code words of weight 12 in GC_{24} are called dodecads.

We may identify a code word $w = (c_0, c_1, ..., c_{23})$ with the set of indices i of the non-zero coordinates $c_i \neq 0$.

Theorem 262. *M_{12} is the stabilizer in M_{24} of a dodecad, regarded as a set of indices.*

13.6 M_{12} is crossing the rubicon

The result of this section was mentioned briefly in §12.3 above.

Let $f_1, f_2, ..., f_{12}$ denote the basic moves ($2\pi/5$ degree turns of a "pentagon" about a vertex) of the Rubik isocahedron, regarded as elements of S_V, where V denotes the set of 12 vertices of the Rubik isocahedron ("rubicon").

The following remarkable result is due to John Conway [CS].

Theorem 263. $M_{12} =< x * y^{-1} \mid x, y \in \{f_1, ..., f_{12}\} >$.

In other words, the Mathieu group M_{12} is generated by the twist-untwist moves of the Rubik isocahedron. If we call a "twist-untwist" move of the form $x * y^{-1}$ (with x, y as in the theorem above) a cross move then (with apologies to Caeser) the theorem above says that M_{12} is generated by the crosses of the rubicon.

In fact, C acts 5-transitively on the set of vertices of the rubicon (this is implicit in [CS]).

13.7 An aside: A pair of cute facts

It's hard to resist stating some more interesting facts about the Mathieu groups.

13.7.1 Hadamard matrices

Let $A = (a_{ij})_{1 \leq i,j \leq n}$ denote a real $n \times n$ matrix. The following question seems quite natural in a course in advanced vector calulus or real analysis:

Question: What is the maximum value of $|\det(A)|$, where the entries of A range over all real numbers $|a_{ij}| \leq 1$?

From vector calculus we know that the absolute value of the determinant of a real square matrix equals the volume of the parallelpiped spanned by the row (or column) vectors of the matrix. The volume of a parallelpiped with sides of a *fixed* length depends on the angles the row vectors make with each other. This volume is maximized when the row vectors are mutually orthogonal, i.e., when the parallelpiped is a cube in $\mathbb{R}^n$. Suppose now that the row vectors of A are all orthogonal. The row vectors of A, $|a_{ij}| \leq 1$, are longest when each $a_{ij} = \pm 1$, which implies that the length of each row vector is $\sqrt{n}$. Suppose, in addition, that the row vectors of A are all of length $\sqrt{n}$. Such a matrix is called a Hadamard matrix of order n. Then $|\det(A)| = (\sqrt{n})^n = n^{n/2}$, since the cube has n sides of length $\sqrt{n}$. Now, if A is any matrix as in the above question then we must have $|\det(A)| \leq n^{n/2}$. This inequality is called Hadamard's inequality.

What is shocking at first (at least to me) is that, there does not always exist a Hadamard matrix. For example, there is a 2×2 Hadamard matrix but not a 3×3 one. What is perhaps even more suprising is that, in spite of the fact that the above question (which is unsolved) arose from an analytic perspective, Hadamard matrices are related more to coding theory, number theory, and combinatorics [vLW]!

Example 264. Let

$$A := \left(\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \end{array}\right)$$

This is a Hadamard matric of order 12.

Exercise 13.7.1. Show that

(a) if you swap two rows or columns of a Hadamard matrix, you will get another Hadamard matrix,

(b) if you multiply any row or column of a Hadamard matrix by -1, you will get another Hadamard matrix,

(c) if you multiply any Hadamard matrix on the left by a signed permutation matrix (that is, a matrix with exactly one ± 1 per row and column) then you will get another Hadamard matrix,

(d) if you multiply any Hadamard matrix on the left by a signed permutation matrix (that is, a matrix with exactly one ± 1 per row and column) then you will get another Hadamard matrix.

Exercise 13.7.2. Let A, B be two Hadamard matrices of order n. Call A, B left equivalent if there is an $n \times n$ signed permutation matrix P such that $A = PB$. Show that this defines an equivalence relation on the set of all Hadamard matrices of order n.

Exercise 13.7.3. Let A be a Hadamard matrix of order n. Let $Aut(A)$ denote the set of all $n \times n$ signed permutation matrices Q such that A is left equivalent to AQ. Show that $Aut(A)$, called the automorphism group of A, is a group under matrix multiplication.

The following result is yet another indication of the unique role of these Mathieu groups in mathematics:

Theorem 265. *(M. Hall, Assmus-Mattson [AM]) Let A be the Hadamard matrix of order 12 in the above example. Then $Aut(A) \cong M_{12}$.*

13.7.2 5-transitivity

The following result exemplifies once more the unique role of these Mathieu groups in group theory:

Theorem 266. *If G is a subgroup of S_X for some finite set X and if G acts 5-transitively on X then exactly one of the following must be true:*

(a) $G \cong S_n$, for some $n > 4$,
(b) $G \cong A_m$, for some $m > 6$,
(c) $G \cong M_{12}$,
(d) $G \cong M_{24}$.

Furthermore, each of the groups in (a)-(d) acts 5-transitively on some finite set.

For a proof of this, see [CS] and [R], ch 9.

Chapter 14

Appendix: Some solution strategies

> "The emphasis on mathematical methods seems to be shifted more towards combinatorics and set theory - and away from the algorithm of diiferential equations which dominates mathematical physics."
>
> *J. von Neumann and O. Morganstern, THEORY OF GAMES AND ECOMONIC BEHAVIOR, 1944*

This chapter includes some strategies for solving the 3x3 Rubik's cube, the 4x4 Rubik's cube, the masterball, the equator puzzle, the skewb, and the pyraminx. For *unexplained notation* used in some of the sections below, see chapter 4.

First (this is a mathematics course, after all!) we discuss some of the mathematical ideas behind the computer algorithms used to study the Rubik's cube:

14.1 The subgroup method

One approach to solve the Rubik's cube using a computer has been to construct a certain sequence of subgroups

$$G_n = \{1\} \ < \ G_{n-1} \ < \ ... \ < \ G_1 \ < \ G_0 = G,$$

where $G =< R, L, F, B, U, D >$ is the Rubik's cube group, which allows the following strategy to be implemented:

- represent a given position of the Rubik's cube by an element $g_0 \in G$,
- determine a complete set of coset representatives of G_{k+1}/G_k:

$$G_{k+1}/G_k = \cup_{i=1}^{r_k} g_{k+1,i} G_{k+1}, \qquad \text{some } r_k > 1, \forall 0 \leq k < n$$

  (note $m_{n-1} = 1, g_{n,1} = 1$),
- (step 1) if $g_0 \in g_{1,i}G_1$ (where $i \in \{1, ..., n_1\}$) then let $g_1 = g_{1,i}$ and $g_1' = g_1^{-1} g_0$ (note $g_1' \in G_1$),
- (inductive step) if $g_k' \in G_k$ has been defined and if $g_k' \in g_{k+1,j} G_k$ (where $j \in \{1, ..., n_1\}$) then let $g_{k+1} = g_{k+1,j}$ and $g_{k+1}' = g_{k+1}^{-1} g_k'$ (note $g_{k+1}' \in G_{k+1}$),
- putting all these together, we obtain $1 = g_n^{-1} g_{n-1}^{-1} g_{n-2}^{-1} ... g_1^{-1} g_0$, so

$$g_0 = g_1 g_2 ... g_{n-1} g_n.$$

The hope is to be able to choose the sequence of subgroups G_i in such a way that the coset representatives are short, relatively simple moves on the Rubik's cube so that the "solution" $g_0 = g_1 g_2 ... g_{n-1} g_n$ is not too long.

14.1.1 Example: the corner-edge method

We now present an example - a fairly unsophisticated one but you will get the idea.

Let G_1 denote the subgroup which does not permute any corners, let G_2 denote the subgroup which does not permute any corners or edges, let G_3 denote the subgroup which does not permute any corners or edges and does not reorient any corners, and let $G_4 = \{1\}$:

$$G_4 = \{1\} \ < \ G_3 \ < \ G_2 \ < \ G_1 \ < \ G_0 = G.$$

This choice of subgroups crudely models the "corner-edge method" (see the appendix) due to Singmaster [Si].

The idea is simple.

1. Represent a given position of the Rubik's cube by an element $g_0 \in G$.

2. Let g_1 denote the move which moves all the corners into the correct positions (i.e., permutes them into the solved position and possibly twists them), so $g_1^{-1} g_0 \in G_1$. Let $g_1' = g_1^{-1} g_0$.

3. Let g_2 denote the move which moves all the edges into the correct positions (i.e., permutes them into the solved position and possibly reorients corners and edges) and leaves all other pieces unpermuted, so $g_2^{-1} g_1' \in G_2$. Let $g_2' = g_2^{-1} g_1'$.

4. Let g_3 denote the move which "solves" all the corners (i.e., twists them all into the correct orientation and may flip some edges) but does not permute any pieces, so $g_3^{-1} g_2' \in G_3$. Let $g_3' = g_3^{-1} g_2'$.

5. Let g_4 denote the move which "solves" all the edges (i.e., flips them all into the correct orientation) and leaves all other facets along.

6. The "solution" is $g_0 = g_1 g_2 g_3 g_4$.

14.1.2 Example: Thistlethwaite's method

Morwen Thistlethwaite (a knot-theorist now at the Univ. of Tennessee) developed one of the best subgroup methods for solving the cube [FS]. He takes

$$G_1 =< R, L, F, B, U^2, D^2 >, \quad G_2 =< R, L, F^2, B^2, U^2, D^2 >,$$
$$G_3 =< R^2, L^2, F^2, B^2, U^2, D^2 >, \quad G_4 = \{1\}.$$

G_2 is isomorphic to the "Rubik's $3 \times 3 \times 2$-domino" group. It's order is $(8!)^2 \cdot 12$, according to [FS], §7.6. G_3 is the "squares" group. It's order is $2^{13} \cdot 3^4$, according to [FS], §7.6.

He has shown (using a computer to help with some of the work) that

- there is a complete set of coset representatives $\{g_{1,i} \mid 1 \leq i \leq n_1\}$ of G/G_1 such that each $g_{1,i}$ is at most 7 moves long (and $n_1 = 2048$),

- there is a complete set of coset representatives $\{g_{2,i} \mid 1 \leq i \leq n_2\}$ of G_1/G_2 such that each $g_{2,i}$ is at most 13 moves long (and $n_2 = 1082565$),

- there is a complete set of coset representatives $\{g_{3,i} \mid 1 \leq i \leq n_3\}$ of G_2/G_3 such that each $g_{3,i}$ is at most 15 moves long (and $n_3 = 29400$),

- there is a complete set of coset representatives $\{g_{4,i} \mid 1 \leq i \leq n_4\}$ of G_3/G_4 such that each $g_{4,i}$ is at most 17 moves long (and $n_4 = 663552$).

Therefore, the Rubik's cube can be solved in at most $7 + 13 + 15 + 17 = 52$ moves.

More recent improvement's on this method have gotten this number down to fourty-something in the "quater-turn metric" I think (see [Lo] for details and recent updates).

14.2 3×3 Rubik's cube

Consider the group $G =< R, L, U, D, F, B >$ of moves of the Rubik's cube. The size of the group generated by these permutations is $43252003274489856000 \cong 4.3 \times 10^{19}$.

14.2.1 Strategy for solving the cube

Let $x^y = y^{-1} * x * y$ denote conjugation and $[x, y] = x * y * x^{-1} * y^{-1}$ denote the commutator, for x, y group elements.

Let M_R denote clockwise (with respect to right side) quarter turn of the middle slice parallel to the right side.

The layer method solution strategy is composed of 3 stages:

Stage 1: Solve the top face and top edges.

Stage 2: Solve the middle edges (and bottom edges as best as possible).

Stage 3: Solve the bottom corners (and bottom edges if necessary).

The corner-edge method solution strategy is composed of 2 stages:

Stage 1: Solve and then orient the corners.

(The move $U * F * [R, U]^3 * F^{-1}$ permutes (ubr,ufl)(uf,ul,ub,ur).)

Stage 2: Solve the and then orient the edges.

"clean" edge and corner moves:

$M_R^2 * U^{-1} * M_R^{-1} * U^2 * M_R * U^{-1} * M_R^2$	edge 3-cycle (uf,ul,ur)
$(M_R * U)^3 * U * (M_R^{-1} * U)^3 * U$	flips the top edges uf, ub
$(R^2 * U^2)^3$	permutes (uf,ub)(fr,br)
$(M_R * U)^4$	flips ub,ul and flips df,db
$(r^{-1} * D^2 * R * B^{-1} * U^2 * B)^2$	ufr+, bld++
$[R, U]^3$	permutes (ufr,dfr)(ubr,ubl)
$F^2 * L^2 * U^2 * (F^2 * L^2)^3 * U^2 * L^2 * F^2$	permutes (uf,ub)(ur,ul)
$(D^2 * R^2 * D^2 * (F^2 * R^2)^2 * U)^2$	permutes (ufl,ubr)(dfr,dbl)
$(M_R^2 * U * M_R^2 * U^2)^2$	permutes (ufl,ubr)(ufr,ubl)
$[R * D * R^{-1}, U]$	corner 3-cycle (brd,urb,ulb)

These moves were compiled with help from the books [Si], [B], [Sn], and [Gap].

14.2.2 Catalog of 3×3 Rubik's "supercube" moves

The supercube is the Rubik's cube with each center facet marked with a short line through it and an adjoining edge.

* $(M_R^2 * U^{-1} * M_R^{-1} * U^2 * M_R * U^{-1} * M_R^2)^2$ is the top edge 3-cycle (uf,ur,ul),

* $(R^{-1} * D^2 * R * B^{-1} * U^2 * B)^2$ twists the ufr corner clockwise and the bld corner counterclockwise (and does not twist any centers).

* $M_R^{-1} * M_D^{-1} * M_R * U^{-1} * M_R^{-1} * M_D * M_R * U$ is the center twist u+, r- (for these last three moves, see [Si], [Sn])

14.3 4×4 Rubik's cube

The solution strategy is composed of 3 stages:
Stage 1: Solve the corners. For this moves for the 3×3 Rubik's cube.
Stage 2: "Pair" the edges so that the neighboring facets on neighboring middle edges have the same color. For this the following "clean edge moves" are useful:

- flipedge:

  $$L_2^2 * D_1^2 * U_2 * F_1^3 * U_2^3 * F_1 * D_1^2 * L_2^2 * L_1 * U_1 * L_1^3 * U_2^3 * L_1 * U_1^3 * L_1^3$$

  (due to J. Adams [A] who calls it "move 8"). This flips and swaps the two middle edge facets on the UF boundary. It affects some centers, but no other edges or corners.

- upedgeswap:

$$R_2 * B_1^2 * D_1^2 * B_1^3 * R_2^3 * B_1 * D_1^2 * B_1^3 * R_2 * B_1^3 * R_2^2$$

  (due to Thai [T], who calls it an "11 gram"). This move affects some centers but no corners and only 4 edge facets. It swaps and flips the right-most UF edge cubie with the left-most (with respect to the B face) UB edge subcube, sending the U facet of the right-most UF edge subcube to the B facet of the left-most UB edge subcube.

- 3-cycle

$$(R_2 * U_1)^3$$

  is a 3 cycle on the edges: (R_2uf, B_2ur, B_2ul). This doesn't affect any other edges and leaves all corners fixed.

Stage 3: Solve the edges. For this the "clean edge moves" for the 3×3 Rubik's cube.
Stage 4: If necessary, apply the flipedge move above,
Stage 5: Solve the centers. For this, use the following "clean center move":

$$center3cycle = R_1^{-1} * F_2 * R_2^{-1} * F_2^{-1} * R_1 * F_2 * R_2 * F_2^{-1}$$

(also called "move 9", due to J. Adams). This move is a 3-cycle on centers facets, affecting no edges, no corners, and no other center facets. It is the 3-cycle (15 19 18) in the above notation.

Some similar clean center moves:

$$center1 = B_1^2 * R_2^3 * F_2 * R_2 * B_1^2 * R_2^3 * F_2^3 * R_2,$$

$$center2 = R_2^2 * B_1^2 * R_2^3 * F_2 * R_2 * B_1^2 * R_2^3 * F_2^3 * R_2^3$$

These aren't really necessary since the the center3cycle can always be applied after a suitable set-up move (i.e., in combination with a suitable conjugation).

The following move is occasionally useful:

$$centerswap = (R_2^2 * U_2^2)^4$$

This affects only 6 center facets (on the front and back faces) and no others. It is the product of two 3-cycles: (15 34 23)(27 14 22) in the above notation.

These moves were compiled with help from the books [A] and [T].

14.4 Rainbow masterball

The solution strategy

Step 1: The idea is to first get all the middle bands aligned first, so you get ball corresponding to a matrix of the form

*	*	*	*	*	*	*	*
1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8
*	*	*	*	*	*	*	*

Here, $*$ denotes any color. We have labeled the colors on the masterball as $1, 2, ..., 8$ in order of occurrence.

We describe a method, which I call "fishing", for achieving this. (Mathematically, this amounts to performing some carefully choosen commutators.) Without too much trouble you can always assume that we have one column aligned. You may need to flip or rotate the ball a little bit to do this. Call this aligned column "column 1" and call the color in column 1, "color 1". We want to get the middle two entries in column 2 aligned. Call the color in the (2,3)-entry "color 2".

We want to get color 2 in the (2,2)-entry. The remaining large color 2 tile is what we will "fish" for. Hold the ball in front of you in such a way that column 2 is slightly to the left of center and column 3 is slightly to the right of center. There are 4 facets in the right upper middle band, 4 facets in the left upper middle band, 4 facets in the right lower middle band and 4 facets in the left lower middle band. A flip about the center on the right half (i.e., perform f_2) exchanges these. We may assume that color 2 is on one of the four facets in the right lower middle band. (If it isn't you need to apply f_2 first). Now perform $r_2^{-1} * f_2^{-1} * r_2 * f_2$: first perform r_2^{-1} (this is "baiting the hook"), then f_2^{-1} ("putting the hook in the water"), then r_2 ("setting the hook"), and finally f_2 ("reeling in the hook"). You may or may not have color 2 in the (2,2) place like you want but the color 1 stripe is intact. If necessary, try again. After at most 4 tries you'll be successful.

Step 2: Repeat this "crab fishing" strategy to get color 2 in the (1,2) position (using $r_1^{-1} * f_2^{-1} * r_1 * f_2$ in place of $r_2^{-1} * f_2^{-1} * r_2 * f_2$). Now, by turning the ball over if necessary, repeat this idea to get color 2 in the (4,2) position. Now you have two "aligned" stripes on your ball - color 1 in column 1 and color 2 in column 2. We say, in this case, that columns 1 and 2 have been "solved".

Step 3: Repeat this for columns 3 and 4.

Step 4: Use the moves in the "catalog" below to finish the puzzle. (I believe the only moves needed are the "equator2swap36" and the "polar2swap36" below, along with suitable cleverly choosen "set-up moves".)

14.4.1 A catalog of rainbow moves

Column moves

We number the columns as 1,...,8. We will use a signed cycle notation to denote an action of a move on the columns of the masterball.

Example 267. A move which switches the 1st and 3rd column but flips both of them over will be denoted by (1 3)$_-$.

A move which sends the 4th column to the 6th column, the 6th column to the 5th column, and switches the 2nd and 3rd column but flips both of them over will be denoted by (2 3)$_-$(6 5 4).

move	cycle
f_1	$(1,4)_-(2,3)_-$
f_2	$(2,5)_-(3,4)_-$
f_3	$(3,6)_-(4,5)_-$
f_4	$(4,7)_-(5,6)_-$
f_5	$(5,8)_-(6,7)_-$
f_6	$(1,6)_-(7,8)_-$
f_7	$(2,7)_-(1,8)_-$
f_8	$(3,8)_-(1,2)_-$
$f_1 * f_2 * f_1$	$(1,2)_-(3,5)$
$f_1 * f_2 * f_1 * f_2$	$(5,4,3,2,1)_-$
$f_1 * f_3 * f_1$	$(1,5)(2,6)$
$f_2 * f_3 * f_2$	$(2,3)_-(6,5,4)$
$f_1 * f_4 * f_1$	$(1,7)(5,6)$
$f_1 * f_5 * f_1$	$(5,8)_-(6,7)_-$
$f_1 * f_8 * f_1$	$(2,8)(3,4)_-$
$f_8 * f_1 * f_8$	$(1,8)_-(4,3,2)$
$f_2 * f_1 * f_2$	$(1,3)(4,5)_-$
$f_3 * f_1 * f_3$	$(1,3)(4,8)_-$
$f_8 * f_1 * f_2$	$(1,4)_-(2,3,8,5)_-$

Finally, $(f_1 * f_2 * f_3 * f_4)^2 * r_1 * r_2 * r_3 * r_4$ swaps the 7,8 columns and leaves all the others fixed but flipped over.

Some products of 2-cycles on the facets

These are all based on an idea of Andrew Southern. The polar2swap and equator2swap were obtained by trying variations of some of Andrew's moves on a MAPLE implementation of the masterball [J].

We number the facets in the i-th column, north-to-south, as $i1, i2, i3, i4$ (where $i = 1, 2, ..., 8$).

move	cycle
$x = r_1 * f_4 * r_1^{-1} * r_4 * f_4 * r_4^{-1}$	(41, 84)(44, 81)
$x * r_1^4 * x * r_4^4$	(41, 81)(44, 84)
$f_1 * r_1 * f_4 * r_1^{-1} * r_4 * f_4 * r_4^{-1} * f_1$	(14, 84)(11, 81)
polar2swap36	(11, 14)(31, 61)
polar2swap18	(61, 64)(11, 81)
equator2swap36	(12, 13)(32, 62)
equator2swap18	(62, 63)(12, 82)

where

$$polar2swap36 = f_1*r_3^{-1}*r_4^{-1}*f_1*f_2*r_1*r_4^{-1}*f_2*r_4^4*f_2*r_1^{-1}*r_4*f_2*r_4^4*f_1*r_3*r_4*f_1$$

(moreover, if you replace r_3 by r_2 both times in this move you get the same effect),

$$polar2swap18 = f_1*r_3^{-1}*r_4^{-1}*f_3*f_4*r_1*r_4^{-1}*f_4*r_4^4*f_4*r_1^{-1}*r_4*f_4*r_4^4*f_3*r_3*r_4*f_1$$

$$equator2swap36 = f_1*r_4^{-1}*r_3^{-1}*f_1*f_2*r_2*r_3^{-1}*f_2*r_3^4*f_2*r_2^{-1}*r_3*f_2*r_3^4*f_1*r_4*r_3*f_1$$

$$equator2swap18 = f_1*r_4^{-1}*r_3^{-1}*f_3*f_4*r_2*r_3^{-1}*f_4*r_3^4*f_4*r_2^{-1}*r_3*f_4*r_3^4*f_3*r_4*r_3*f_1$$

For further details on the rainbow puzzle, see [JS], [J].

14.5 Equator puzzle

Solution strategy, in brief:

- First, ignore the orientation of the pieces. Just try to get the pieces in their correct position. One of the most remarkable properties of this puzzle is that GAP [Gap] is, in practice, very efficient at solving this part of the solution. (This is remarkable in view of the fact that GAP is not very good at solving the corresponding problem for the Rubik's cube, for example, so there is no reason to expect it to be good at solving this problem.)
- Second, once the pieces are in the correct position, they must be correctly oriented by a catalog of "node" moves designed for that purpose. Some "node" moves are included below.

Some notation: if x, y, and z are moves, let

$$[x, y, z] = x^{-1} * y^{-1} * z^{-1} * x * y * z.$$

Example 268. Some moves discovered using GAP:

- $[r_1^{-3}, r_2^{-3}, r_3^{-3}]$ will swap the NP and SP, while rotating the NP by 90 degrees in a counter clockwise direction. Moreover, it will fix the position of the piece labeled as 20 but will rotate it by 90 degrees clockwise.
- To send 1 (the NP) to 4, 4 to 7 (the SP), 7 to 10, and 10 to 1:

$$(1, 4, 7, 10) = (r_2^{-1} * r_3^{-1} * r_1^2 * r_3^2 * (r_3^{-1} * r_1^{-1})^2 * r_3 * r_2 * r_1^{-3})^2 * r_1^5$$

- The *square* of the previous move is easier to do:

$$(1, 7)(4, 10) = r_1^3 * r_2^6 * r_1^{-3} * r_2^{-6}$$

- a 3-cycle about the NP and then a 3-cycle about the SP:

$$(2, 22, 12)(6, 8, 17) = r_1 * r_2 * r_1^{-1} * r_2^{-1} * r_2 * r_1^{-1} * r_2^{-1} * r_1$$

- if rot_{90} denotes a 90^o solid rotation,

$$rot_{90} = (2, 13, 12, 22)(3, 14, 11, 21)(5, 16, 9, 19)(6, 17, 8, 18) * r_3^{-1},$$

then the following move will exchange two pairs of facets neighboring the NP and two pairs of facets neighboring the SP:

$$(2, 12)(6, 8)(13, 22)(17, 18) = (r_1 * r_2 * r_1^{-1} * r_2^{-1} * r_2 * r_1^{-1} * r_2^{-1} * r_1) * rot_{90} *$$
$$*(r_1 * r_2 * r_1^{-1} * r_2^{-1} * r_2 * r_1^{-1} * r_2^{-1} * r_1) * rot_{90}^{-1}$$

- A single 2-cycle or 3-cycle cannot be achieved in the group generated by r_1, r_2, r_3.

We call a move of the form $[r_1^{3k}, r_2^{3m}, r_3^{3n}]$ a node move since it only affects the nodes (where the circles intersect). The table below records where each node goes as well as its effect on the orientation. The position entry in a block is the position the piece moves to. The angle entry, if any is the angle the piece gets rotated by. No angle entry means, of course, that the piece is not rotated. No position entry means that the piece was not moved (but may have been rotated). If a move has no effect on the position or the angle then we fill in the block with a "-".

In the following table, NP, SP have been denoted by 1,7, resp., for brevity.

move,piece	1	7	4	10	15	20
m123	7,90ccw	1,90cw	10,180	4,180	90ccw	90cw
m132	7,180	1,180	90ccw	90cw	20,90cw	15,90ccw
m231	7,180	1,180	90cw	90ccw	20,90cw	15,90ccw
m213	90cw	90ccw	10,90cw	4,90ccw	20	15
m312	90ccw	90cw	10,90cw	4,90ccw	20	15
m321	7,90ccw	1,90cw	10,180	4,180	90cw	90ccw
A	180	180	180	180	-	-
$m321^2$	-	-	-	-	180	180
B	-	-	180	180	-	-
n123	1,90ccw	7,90cw	10	4	20,90ccw	15,90cw
D	-	-	90cw	90ccw	90cw	90ccw

where

$$\begin{gathered} m123 = [r_1^{-3}, r_2^{-3}, r_3^{-3}], \\ m132 = [r_1^{-3}, r_3^{-3}, r_2^{-3}], \\ m231 = [r_2^{-3}, r_3^{-3}, r_1^{-3}], \\ m213 = [r_2^{-3}, r_1^{-3}, r_3^{-3}], \\ A = m123 * m132 * m213, \\ B = C * m321^2 * C^{-1}, C = (1\ 4)(7\ 10) = r_1^3, \\ n123 = [r_1^{-3}, r_2^{-3}, r_3^3], \\ D = [r_1^{-3}, r_2^{-3}, r_3^3]. \end{gathered}$$

Remark 26. Let G denote the subgroup of S_{30} generated by r_1, r_2, r_3. According to GAP [Gap],

$$|G| = 21424936845312000 = 15! \cdot 2^{14} = (2.14...) \cdot 10^{16}.$$

The largest normal subgroup of G which is a power of 2 is of order 2^{14}. Furthermore, G appears to act transitively on the following 15 pairs of facets:

$$B = \{[1,7],[2,8],[13,18],[3,9],[14,19],[4,10],[15,20],[5,11],$$

$$[23,27],[16,21],[25,29],[6,12],[24,28],[17,22],[26,30]\}.$$

Possibly G is isomorphic to a semidirect product of $S_B \cong S_{15}$ acting on C_2^{14}.

14.6 The skewb

14.6.1 Strategy

The goal here is to collect enough moves to support the following solution strategy: fix the centers and solve the corners using "clean corner moves" (i.e., moves which do not effect the centers).

The basic moves are twists by 120 degrees clockwise about each of the six corners FRU,FLU,BRU,BLU,BDR,BDL,DFR,DFL.

14.6.2 A catalog of skewb moves

Thanks to J. Montague and G. Gomes for comments and corrections for the descriptions below, which were discovered with the help of a simulation of the skewb written for MAPLE [Jwww].

1. $FRU * BLU * FRU^{-1}$ is order 3.

2. $[FRU * FLU]^3$ twists 6 corners clockwise by 120 degrees. The 2 corners not twisted are those opposite the FRU, FLU corners: the BDR, BDL corners. The centers are all fixed. $(FRU * FLU)^3 = (FLU * FRU)^3$ rotates all the corners except for the bd corners. It does not permute any facets.

3. The move, $[FRU * BLU]^5$, fixes all the centers and the 2 "opposite" corners: DFL, BDR. It twists the 3 corners FLU, BLU, and FRU. On the remaining 3 corners, it acts as the permutation (DFR, BRU, BDL).

4. FRU = BDL (actually, they are only equal up to a rotation of the entire cube). In general, a corner move is equal to the opposite corner move up to a rotation of the entire cube.

5. $(FRU * FLU)^3 * (BDL * BDR)^6$ rotates all the corners except for the bu and the df corners. The uf corners are rotated clockwise and the bd corners counterclockwise. It does not permute any facets. $(FRU * FLU)^6 * (BDL * BDR)^3$ is the same move, but rotates in the opposite direction.

6. $(FRU * FLU)^6 * (BDL * BDR)^6$ rotates the corners as follows:

   - the uf corners counterclockwise,
   - the db corners counterclockwise,
   - the df corners clockwise,
   - the ub corners clockwise.

   It does not permute any facets.

7. Let $bottomspin = (FRU * FLU)^6 * (BDL * BDR)^3 * (DFR * DFL)^3$. This move rotates the 4 bottom corners (the df corners clockwise and the db counterclockwise). It does not permute any facets.

8. $(BRU * FLU)^9$ is a 5 cycle on the center facets (F, R, B, U, L). It fixes the bottom and does not affect any corners. $(BLU * FRU)^9$ is a 5 cycle on the center facets. It fixes the bottom and does not affect any corners.

9. $(BLU * FRU)^9 * (BRU * FLU)^9$ is a product of 2 transpositions on the center facets, swapping front/back and up/right. It fixes the bottom and does not affect any corners.

10. Let U denote the clockwise (with respect to the up face) rotation of entire cube by 90 degrees. Then $bottomspin * U * bottomspin$ rotates but does not swap 2 corners (the DFR and BDL) and does not affect any other corners or faces.

14.7 The pyraminx

Assume that the tetrahedron is lying on a flat surface in front of you, with the triangle base pointing away from you. The corners are denoted L (left), R (right), U (up), and B (back).

Basic Moves: Let

- L denote the 120 degree clockwise rotation of the 2-level subtetrahedron containing the left corner,
- R denote the 120 degree clockwise rotation of the 2-level subtetrahedron containing the right corner,
- U denote the 120 degree clockwise rotation of the 2-level subtetrahedron containing the up corner,
- B denote the 120 degree clockwise rotation of the 2-level subtetrahedron containing the back corner.

First, get the "center" facets solved, then twist the corner tips to solve them and the center facets. Finally, to solve the edge facets, use the following moves (given in [EK]):

- $[R, U^{-1}]$ is a 3-cycle of edge pieces on the URL face,
- $[R, U^{-1}] * [R^{-1}, L]$ is a flip of two edges (UR edge and UL edge) on the URL face.

14.8 The megaminx

The strategy here is the same as for the 3x3 Rubik's cube:

- place the corners correctly first (ignoring correct corner orientation),
- place the edges correctly first (ignoring correct edge orientation),
- twist the corners if necesary,
- flip the edges if necessary.

Moves useful for carrying out these steps are included in the following catalog.

14.8.1 Catalog of moves

First, some notation. We label the faces $f_1, f_2, ..., f_6$ on top and label the bottom faces $f_7, f_8, ..., f_{12}$ as in chapter 4. The same notation is used to indicate the move of the megaminx given by rotating that face of the megaminx by 72 degrees clockwise.

- $f_1^{-1} * f_2^{-1} * f_1 * f_2 * f_1^{-1} * f_2^{-1} * f_1 * f_2 * f_1^{-1} * f_2^{-1} * f_1 * f_2 = [f_1, f_2]^3$ swaps the $f_1.f_3$ and the $f_2.f_6$ corners: $(f_1.f_2.f_3, f_1.f_3.f_4)(f_1.f_2.f_6, f_2.f_6.f_7)$
- $m = f_3 * f_6^{-1} * f_4 * f_2^{-1} * f_5 * f_3^{-1} * f_6 * f_4^{-1} * f_2 * f_5^{-1}; f_6 * f_1 * m^6 * f_1^{-1} * f_6^{-1}$ swaps 2 pairs of corners on the f_1 face: $(f_1.f_2.f_6, f_1.f_3.f_4)(f_1.f_2.f_3, f_1.f_5.f_6)$
- $f_1 * f_6 * f_1^{-1} * f_2 * f_1 * f_6^{-1} * f_1^{-1} * f_2^{-1}$ 3 cycle on corners and 3-cycle on edges $(f_1.f_2.f_6, f_1 1.f_7.f_6, f_2.f_6.f_7)(f_1.f_2, f_6.f_7, f_2.f_6)$
- $M2 = f_6 * f_2 * f_1 * f_2^{-1} * f_1^{-1} * f_6^{-1} * f_3^{-1} * f_1^{-1} * f_2^{-1} * f_1 * f_2 * f_3$ (Mark Longridge) edge 3-cycle $(f_1.f_2, f_2.f_3, f_2.f_6)$
- $(f_6^{-1} * f_2^{-1} * f_3^{-1} * f_6 * f_2 * f_3)^6$ - triple corner twister, ccw twists of $f_1.f_2.f_3, f_1.f_2.f_6, f_1.f_5.f_6$
- $M3 = f_3^(-2) * f_6^2 * f_2 * f_1^{-1} * f_6 * f_1 * f_3^2 * f_6^2 * f_1 * f_6^{-2} * f_3^{-2} * f_1^{-1} * f_6^{-1} * f_1 * f_2^{-1} * f_6^{-2} * f_3^2 * f_1^{-1}$ (Mark Longridge) edge 2-flip of $f_1.f_2, f_1.f_6$
- $M3a = f_6^{-1} * f_2^{-1} * f_1 * f_3^{-1} * f_1^{-1} * f_3 * f_2 * f_6 * f_3 * f_2 * f_1^{-1} * f_6 * f_1 * f_6^{-1} * f_2^{-1} * f_3^{-1}$ (Mark Longridge) edge 2-flip of $f_1.f_2, f_1.f_3$

For further details, see the internet sites [J] or [Lo].

Bibliography

[A] J. Adams, HOW TO SOLVE RUBIK'S REVENGE, Dial Press, NY, 1982

[Are] Andrew Arensburger, Square 1. http://www.cfar.umd.edu/~arensb/Square1/

[Ar] M. Artin, ALGEBRA, Prentice-Hall, 1991

[AM] E. Assmus, Jr. and H. Mattson, "On the auotmorphism groups of Paley-Hadamard matrices", in COMBINATORIAL MATHEMATICS AND ITS APPLICATIONS, ed. R. Bose, T. Dowling, Univ of North Carolina Press, Chapel Hill, 1969

[Ba] J. Baez, "Some thoughts on the number 6", internet newsgroup sci.math article, posted May 22, 1992, http://math.ucr.edu/home/baez/README.html

[B] C. Bandelow, INSIDE RUBIK'S CUBE AND BEYOND, Birkhauser Boston, 1980

[BCG] Berlekamp, J. Conway, R. Guy, WINNING WAYS, II, Academic Press,

[BH] R. Banerji and D. Hecker, "The slice group in Rubik's cube", Math. Mag. 58(1985) 211–218

[Bu] G. Butler, FUNDAMENTAL ALGORITHMS FOR PERMUTATION GROUPS, Springer-Verlag, Lecture Notes in Computer Science, 559, 1991

[Car] R. Carter, SIMPLE GROUPS OF LIE TYPE, Wiley, 1972

[CD] M. Conrady and M. Dunivan, "The Cross Group of the Rubik's Cube", SM485C project, April,1997

[CS] J. Conway and N. Sloane, SPHERE PACKINGS, LATTICES, AND GROUPS, Springer-Verlag, 1993

[CFS] G. Cooperman, L. Finkelstein and N. Sarawagi, "Applications of Cayley graphs", in APPLIED ALGEBRA ..., Springer-Verlag, Lecture Notes in Computer Science, 508, 1990

[C] J. Crossley, et al, WHAT IS MATHEMATICAL LOGIC?, Dover, 1972

[CL] ftp archives of the "cube-lovers" list at `ftp://ftp.ai.mit.edu/pub/cube-lovers/`

[CG] S. Curran and J. Gallian, "Hamiltonian cycles and paths in Cayley graphs and diagraphs - survey", Discrete Math. 156(1996) 1–18

[DM] J. Davies and A. O. Morris, "The schur multiplier of the generalized symmetric group", J. London Math. Soc. 8(1974) 615–620

[DL] M. Dunbar and A. Luers, "The Group Structure of the 2x2 Rubik's Cube", SM485 term paper, Fall 1996

[EK] J. Ewing and C. Kosniowski, PUZZLE IT OUT, CUBES, GROUPS, AND PUZZLES, Cambridge Univ Press, 1982

[FH] W. Fulton and J. Harris, REPRESENTATION THEORY, Springer-verlag, 1991

[FS] A. Frey and D. Singmaster, HANDBOOK OF CUBIK MATH, Enslow Pub., 1982

[G] A. Gaglione, AN INTRODUCTION TO GROUP THEORY, NRL, 1992

[Gap] Martin Schönert et al, GAP MANUAL, Lehrstuhl D für Mathematik, RWTH Aachen

[GJ] M. Garey and D. Johnson, COMPUTERS AND INTRACTIBILITY, W. H. Freeman, New York, 1979

[Gar1] M. Gardner, "Combinatorial card problems" in TIME TRAVEL AND OTHER MATHEMATICAL BEWILDERMENTS, W. H. Freeman, New York, 1988

[Gar2] M. Gardner, MY BEST MATHEMATICAL AND LOGIC PUZZLES, Dover, New York, 1994

[GT] K. Gold, E. Turner, "Rubik's group", Amer. Math. Monthly, 92(1985) 617–629

[GM] G. Gomes and J. Montague, "The skewb group", SM485C project, April,1997

[HR] G. Hardy and S. Ramanujan, "Asymptotic formulae in combinatory analysis", Proc. London Math. Soc. 17(1918)75–115

[H] D. Hofstadler, METAMATHEMATICAL THEMAS, Basics Books, 1985 (Mostly a collection of Scientific American columns he wrote; the articles referred to here were also published in Scientific American, March 1981, July 1982)

[Hum] J. Humphreys, REFLECTION GROUPS AND COXETER GROUPS, Cambridge Univ Press, 1990

[I] J. Isbell, "The Gordon game of a finite group", Amer. Math. Monthly 99(1992)567–569

[J] D. Joyner, "Rainbow masterball page", internet www page http://www.nadn.navy.mil/MathDept/wdj/mball/rainbow.html

[Jwww] D. Joyner, "Permutation puzzle page", internet www page http://www.nadn.navy.mil/MathDept/wdj/rubik.html

[JM] D. Joyner and J. McShea, "The homology group of the square 1 puzzle", preprint

[JN] D. Joyner and G. Nakos, LINEAR ALGEBRA AND APPLICATIONS, to be published (PW+S, 1998?)

[JS] D. Joyner and A. Southern, "The masterball puzzle", preprint

[Ki] A. Kirillov, ELEMENTS OF THE THEORY OF REPRESENTATIONS, Springer-Verlag, 1976

[K] B. Kostant, "The graph of the truncated icosahedron and the last letter of Galois", Notices of the A.M.S. 42(1995)959–968

[L] M. E. Larsen, "Rubik's revenge: the group theoretical solution", Amer. Math. Monthly, 92(1985)381–390

[Lo] M. Longridge, "God's Algorithm Calculations for Rubik's Cube, Rubik's Subgroups, and Related Puzzles", http://web.idirect.com/~cubeman/

[Lu] A. Luers, "The group structure of the pyraminx and the dodecahedral faces of M_{12}", USNA Honors thesis, 1997 (Advisor W. D. Joyner) http://web.usna.navy.mil/~wdj/m_12.htm

[Ma] G. Mackey, UNITARY GROUP REPRESENTATIONS IN PHYSICS, PROBABILITY, AND NUMBER THEORY, Math Lecture Notes Series, Benjamin/Cummins, 1978

[MKS] W. Magnus, A. Karrus and D. Solitar, Combinatorial Group Theory, 2nd ed, Dover, 1976

[Mc] J. McShea, "The 14-15 Puzzle, and Why It Can't Be Solved", SM485 term paper, Fall 1996

[M] R. E. Moritz, MEMORABILIA MATHEMATICA, MacMillan Co, NY, 1914

[NST] P. Neumann, G. Stoy and E. Thompson, GROUPS AND GEOMETRY, Oxford Univ. Press, 1994

[OR] J. O'Connor, E. F. Robertson MacTutor History of Mathematics archive, http://www-groups.dcs.st-and.ac.uk/~history/Information.html

[Rob] S. Robinson, "The Mathematics of Bell Ringing", capstone paper (Advisor W. D. Joyner)

[R] J. J. Rotman, AN INTRODUCTION TO THE THEORY OF GROUPS, 4th ed, Springer-Verlag, Grad Texts in Math 148, 1995

[Ru] E. Rubik, et al, RUBIK'S CUBIC COMPENDIUM, Oxford Univ Press, 1987

[S] R. Schmalz, OUT OF THE MOUTHS OF MATHEMATICIANS, Math. Assoc. Amer., 1993

[Se] J.-P. Serre, LINEAR REPRESENTATIONS OF FINITE GROUPS, Springer-Verlag, 1977

[Ser] J.-P. Serre, TREES, Springer-Verlag, 1980

[Si] D. Singmaster, NOTES ON RUBIK'S MAGIC CUBE, Enslow, 1981

[Sn] R. Snyder, GET CUBED

[Sn2] R. Snyder, TURN TO SQUARE 1, 1993

[St] R. Stoll, SET THEORY AND LOGIC, Dover, 1963

[TW] A. D. Thomas and G. V. Wood, GROUP TABLES, Shiva Publishing Ltd, Kent, UK, 1980

[T] Thai, "The winning solution to Rubik's Revenge", Banbury Books, 1982

[vLW] J. van Lint and R. M. Wilson, A COURSE IN COMBINATORICS, Cambridge Univ. Press, 1992

[Wa] H. B. Walters, CHURCH BELLS OF ENGLAND, Oxford Univ Press, 1912

[Wh] White, Arthur, "Fabian Stedman: The First Group Theorist?", American Mathematical Monthly, Nov. 1996, pp. 771–8.

[W] R. M. Wilson, "Graph puzzles, homotopy, and the alternating group", J. of Combin. Theory, 16 (1974) 86–96